Wi-Fi Install, Configure, and Use 802.11b Wireless Networking

Wi-Fi

——安装、配置和使用 802.11b 无线网络

(美) John Ross 著
王海涛 汤平杨 译

清华大学出版社

Wi-Fi Install, Configure, and Use

802.11b Wireless Networking

无线联网真的难如登天吗？事实并非如此。通过学习本书，您就能轻松掌握这种高速、低成本且功能强大的优秀技术。本书采用深入浅出的语言详细介绍了无线联网技术，读者通过本书可了解到如何安装、配置和使用 802.11b 无线网络，实现安全使用网络的目的。

本书主要内容

- 选择合适的位置设置接入点，以提高网络性能
- 扩展自己的网络，与邻里分享公共或专用无线 Internet 接入
- 设计和使用点对点的无线网络链接，跨数英里范围传输数据
- 找到公共网络，并在旅店、会议中心和机场候机大厅体验网上冲浪
- 使用嗅探工具找到未受保护的无线网络
- 通过加密、密码保护和虚拟专用网(VPN)等措施保护接入点的安全

作者简介

John Ross 有着 20 多年的计算机、数据网络和通信书籍的编写经验，曾出版了 20 多本相关图书。同时，他还为几家知名制造商(包括 Motorola 和 AT&T)提供无线和有线网络的技术咨询服务。

适用于 Windows, Macintosh, Linux, Unix 和 PDA

ISBN 7-302-07991-9

9 787302 079910 >

定价：35.00 元

Wi-Fi

—— 安装、配置和使用 802.11b 无线网络

(美) John Ross 著

王海涛 汤平杨 译

清华大学出版社

北 京

内 容 简 介

以往无线局域网的缺点主要是传输速率低、成本高、产品系列有限且很多产品不能相互兼容。IEEE 802.11b 从根本上改变了无线局域网的设计和应用现状，802.11b 无线局域网由于其便利性和可伸缩性，特别适用于小型办公场所和家庭网络。

本书首先介绍 Wi-Fi 技术的工作原理以及实现无线所需的设备，然后深入分析在运行不同操作系统的计算机上安装和使用无线网络的方法，并介绍一些其他类型的网络，最后讨论相关的安全问题和虚拟专用网(VPN)。

本书适合于需要安装和使用无线网络并且希望更深入研究无线网络的用户，也适合于对无线网络技术感兴趣的读者。

John Ross
Wi-Fi: Install, Configure, and Use 802.11b Wireless Networking
EISBN：1-886411-45-X

北京市版权局著作权合同登记号 图字：01-2003-5400

图书在版编目(CIP)数据

Wi-Fi——安装、配置和使用 802.11b 无线网络/(美)罗斯(Ross，J.)著；王海涛，汤平杨译.
—北京：清华大学出版社，2003
书名原文：Wi-Fi: Install, Configure, and Use 802.11b Wireless Networking
ISBN 7-302-07991-9

Ⅰ.W… Ⅱ.①罗…②王…③汤… Ⅲ.计算机网络—基本知识 Ⅳ.TP393

中国版本图书馆 CIP 数据核字(2004)第 004268 号

出 版 者：清华大学出版社 **地 址**：北京清华大学学研大厦
http://www.tup.com.cn **邮 编**：100084
社 总 机：010-62770175 **客户服务**：010-62776969

组稿编辑：曹康
文稿编辑：李阳
封面设计：康博
版式设计：康博
印 刷 者：北京密云胶印厂
装 订 者：三河市金元装订厂
发 行 者：新华书店总店北京发行所
开 本：185×260 **印张**：14.75 **字数**：307 千字
版 次：2004 年 3 月第 1 版 2004 年 3 月第 1 次印刷
书 号：ISBN 7-302-07991-9/TP·5790
印 数：1～3000
定 价：35.00 元

前　言

通过本地计算机之间的无线连接和 Internet 无线接入两个步骤，Internet 将最终控制世间所有事物。来自于建筑物中任意地方的，乃至于不需要接入电线的整个校园或办公区的可用连接，都可使网络和连接网络的工具更为灵活。在您外出时，从咖啡厅、机场或会议中心到 Internet 的快速接入可以改变您的工作和在线游戏方式。

本书将帮助您了解当前最流行的无线以太网系统 802.11b 或 Wi-Fi。如果您需要在家中、办公室和公共场合安装和使用无线网络，本书将指导您选择和安装网络适配器、基站和天线。本书介绍在运行 Microsoft Windows、Macintosh、Linux 和 Unix 的计算机中使用 Wi-Fi 网络的相关信息；讨论如何将运行不同操作系统的计算机连接到单个网络；分析在安装好无线网络后如何很好地利用它，以及如何处理与操作无线网络相关的安全问题。

在阅读本书时，希望您牢记，一个理想无线网络应当是绝对不可见的网络——一旦该无线网络建立并运行起来，您就不需再考虑它了；您真正要做的应当是交换消息或查看 Web 站点上的内容，而不是扭动天线或改变密钥。对于无线网络来说，任何类型的计算机或网络都是工具，而不是最终产品。记住，您最初的目的是查看 Red Sox 是否获胜、邀请朋友参加一个宴会、阅读课堂笔记或收听苏格兰的广播电台。Internet 无线连接是一个到达终点的方法，但这并不是最终目标。

如果其他类型的网络可以工作得更好，那就没有必要安装无线网络。有线连接、无线连接或通过信使连接都是可选项，您只要做自己想做的就可以了。

同样重要的是，您必须始终控制无线连接。计算机和网络应当按照您需要的方式进行各种工作，而不是调整自己的生活或工作节奏来满足机器的需要。如果您在使 Wi-Fi 网络(或其他与计算机相关的功能)正确工作时遇到了麻烦，则一般都是计算机产生了错误，或是设计硬件和软件的人的错误。您应当以主人而不是佣人的身份出现。

无线网络是一门不断发展的技术，因此本书中的相关信息只能代表当前内容——在不久的将来，一些硬件生产商和无线网络服务供应商将合并或停业，而其他一些将公开数以百计的新热点。性能更高 802.11a 基站和网络适配器将通过网络以更快的速度传输数据，而新的安全标准将使无线网络更难被解密。但是，本书中所描述的一般性原理将不会改变；您依然需要了解如何将计算机配置成通过无线网络发送和接收数据，以及如何将可使用无线网络的计算机从一个网络移到另一个网络。要了解无线网络的新特性和功能，请访问网络硬件生产商的市场宣传和 Web 站点以及第三方的 Web 站点，例如 802.11b Networking News 站点(http://802.11b.weblogger.com/)。

希望本书能为使用 Wi-Fi 网络的人提供更多参考。本书试图包括安装和使用网络的所有必需信息，但当网络建立并运行起来后，您就不用再考虑它了，只需启动计算机，然后开始使用网络交换数据和消息即可。通过阅读本书(即使跳过不感兴趣的章节)，您可以更好地了解 Wi-Fi 的工作原理，并且可以比其他人更好地利用无线网络。本书确实值得您花费更多时间认真钻研。

目　　录

第1章　Wi-Fi的工作原理

确切地说，无线网络可以被看成是一些黑匣子，您可以不用去管它们内部的实现细节就可以对它们进行开启和使用。这其实就是与大多数人关系紧密的 Wi-Fi 技术的工作方式——您不必考虑 802.11b 规范是如何把您的笔记本电脑连接到网络上的。在理想的世界里，只要打开电源开关，Wi-Fi 就已经在工作了。

但是，今天的无线网络的情形如同 1923 年的无线电广播。虽然这种技术已经存在，但人们还不得不把大多数时间花在设备开发上。那些懂得在 Bakelite-Dilecto 面板(如图 1-1 所示)后面究竟发生什么的人们跟只懂把电源开关打开后收听的人相比，显然能从无线电广播中获得更好的性能。

图 1-1　任何新技术都要经过 Tweak-Fiddle 阶段

为了更好地利用无线网络技术，您就应该设法去了解在这个黑匣子里面(或者是组成这个网络的众多黑匣子里面)到底发生什么。本章要描述控制着这些无线网络的标准和规范，另外还要说明数据是如何通过网络在计算机间传输的。

当网络正常工作时，您可以不用去想这个网络通道的内部原理，只要单击计算机屏幕上的几个图标就能连到网络上。但当您试图设计和新建一个网络，或者想调节现有

网络的性能时，就有必要了解一下数据如何能像假定的那样在两地之间传输。当网络中发生了您并不想发生的事件时，您就更应该掌握这种技术的基础知识来解决可能发生的问题。

通过无线网络传输的数据包含三个独立元素：无线电信号、数据格式和网络结构。上述三个部分相互独立，所以在您开发网络时必须一起定义它们。根据人们熟知的OSI(开放系统互联)参考模型，无线电信号发生在物理层，数据格式控制了一些高层，而网络结构则包括了负责发送和接收无线电信号的接口适配器和基站。

在无线网络中，计算机中的网络适配器将数字信号转换成模拟信号，这样信号就可以通过网络上的其他设备进行传输。另外，适配器还将来自其他网络设备的模拟信号转换成数字信号。IEEE(电气电子工程协会)已经出台了一系列“IEEE 802.11”无线网络的标准和规范，通过这些规范定义了上面提到的两种信号的格式和结构。

最初的 802.11 标准(没有以“b”结尾的标准)是在 1997 年制定的。它适用于多种不同的无线媒体：两种不同的无线电传输(下面将详细介绍)和用红外线作媒介的网络。最近的 802.11b 标准为无线以太网提供附加规范。相关的 802.11a 文档谈到以不同的无线电频率进行更高速运作的无线网络，另外还有一些面向公众版本的 802.11 无线电网络标准。

现在使用最广泛的规范则是 802.11b。它事实上是您可能在办公室、公共场所或者家庭遇到的无线以太局域网里最常用的标准。尽管存在很多其他标准，但由于 802.11b 使用最广泛，当您期望连接到网络却不想搞懂如何操作硬件设备时，更是如此。所以，本书将使用该标准。

注意：

本书描述的无线网络都遵循 802.11b 标准，但大多数信息都可应用于其他类型的 802.11 网络。

下面介绍在无线局域网标准中必须了解的其他两个名词：WECA 和 Wi-Fi。WECA(Wireless Ethernet Compatibility Alliance，无线以太网兼容性联盟)是一个由生产符合 802.11b 标准的设备的生产商组成的行业组织。他们的任务有两个方面：首先是测试和认证由他们的成员公司生产的无线网络设备是否能在同一网络中很好地协作，另外就是负责将 802.11b 网络发展成无线局域网的世界级标准。WECA 组织的市场部门则为 802.11 规范采用了较友好的名称 Wi-Fi(Wireless Fidelity 的英文缩略语)，同时还把自己的名称改成了 Wi-Fi 联盟。

这个联盟每年举行一到两次“相互协作研讨会”，这样可使来自很多硬件厂商的工程师们聚集到一起，验证他们的产品是否能正确地与其他生产商的产品进行通信。印有 Wi-Fi 标志的网络设备则表示通过了相关标准的验证，并通过了相互之间的协作测试。图 1-2 显示了印有 Wi-Fi 标志的两个不同厂家生产的网络适配器。

图 1-2　印有 Wi-Fi 标志的网络适配器

1.1　无线电信号

802.11b 网络使用的是 2.4GHz 左右的特殊波段无线电频率，这个波段在世界上大多数国家都被保留用作无许可(unlicensed)的点对点扩频无线电服务。

“无许可”意味着任何使用符合技术要求的设备的人都可以使用这些频率发送和接收无线电信号，而不用得到无线电台的许可。大多数无线电服务都要求许可，将某个频率的专用权授予单个用户或是用户组，而且把该频率的使用局限在一个特殊服务类型里，而无许可的服务与之不同，它是一种全自由方式的服务，每个用户都可以平等地使用同一频段。从理论上讲，这种扩频无线电技术可使其他使用者(点)共存而且没有明显干扰。

点对点的无线电服务运行一个将信息从发射器运送到单个接收器的通信通道。与点对点的无线电服务相反，广播服务(例如电台或电视台)则同时将信号发送到多个接收器。

扩频(spread spectrum)是指使用一个相对较宽的无线电频段传输单个无线电信号的一组方法。无线以太网使用两种不同扩频无线电传输系统：FHSS(frequency-hopping spread spectrum，跳频扩频)和 DSSS(direct-sequence spread spectrum，直序扩频)。一些老的 802.11 网络使用较慢的 FHSS 系统，但现在的 802.11a 和 802.11b 标准的网络都使用 DSSS。

扩频无线电比只使用单一窄通道的其他无线电信号类型多了一些重要功能。扩频特别有效，这样信号发射器可工作在很低功率下。因为工作在一个较宽的频段，这些频道对来自其他无线电信号或电器噪声的干扰的灵敏度就较低，这也意味着这些信号可以在平常窄波段的信号不能接收和理解的环境下顺利传输。另外，由于跳频扩频信号

在多个频道间跳换，这样就使得未授权的接收器很难截获和解码信号的内容。

扩频无线电技术有一段有趣的历史。女演员 Hedy Lamarr 和美国前卫派作曲家 George Antheil 在一个为了控制不易被敌人干扰的、无线电控制的鱼雷的“秘密通信系统”中发明了这种技术。在她去好莱坞之前，她已经和奥地利的一个武器军火商结了婚，从她丈夫客户的晚会那儿她了解到鱼雷导向的一些细节问题。数年后，在二次大战期间，她逐渐有了依靠改变无线电频率来排除干扰的想法。

Antheil 则是把这个思想变成现实的理想人选。他最著名的名为 Ballet Mechanique 的作品则是由 16 架自动钢琴、两个飞机推进器、四架木琴、四个低音鼓和一个警报器共同谱写完成的。他用早先用于同步钢琴的相同方法改变了扩频传输中无线电频率。早先的槽形纸带系统有 88 个无线电频道——每一个频道对应钢琴上的 88 个按键。

理论上，这种方法也可以用于声音和数据通信以及鱼雷导向，但在那个真空管、纸带机和机械同步的时代，整个过程会因为太复杂而实际难以被建立和使用。到了 1962 年，半导体技术替代了真空管和钢琴组，并且这种技术在古巴导弹危机事件中被美国海军舰队用于保护通信。现在，扩频无线电还被用于美国空军太空指挥部的 Milstar(军事星系统)卫星的通信系统、数字蜂窝移动电话和无线数据网络中。

1.1.1 FHSS

Lamarr 和 Antheil 早先设计的扩频无线电使用了一种跳频系统。顾名思义，FHSS 技术将一个无线电信号分成小段，在传输这些信号段时，每秒钟多次从一个频率跳换到另一个频率。发射器和接收器建立了一个同步跳换模式，这一模式可设置他们将使用的不同子频道的序列顺序。

FHSS 系统通过使用一秒钟多次改变频率的窄载波信号，克服了来自其他用户的干扰。同时，其他发射器和接收器也可以同时在同一组子频道上使用不同跳频模式。在任意时间点，每次发射可能使用一个不同的子频道，这样信号之间就不会有干扰。如果发生冲突，系统就会重新发送包，直到接收器获得一个清晰的副本，然后往发射站返回一个确认信息。

对于无线数据服务来说，无许可的 2.4GHz 频带被分成 75 个子频道，每个子频道 1MHz 宽。由于每次频率跳换都会增加数据流的开销，因此 FHSS 发射就相对较慢。

1.1.2 DSSS

DSSS 技术使用了一个 11 片 Barker 序列的方法来扩展无线电信号，它使用了单个 22MHz 宽的频道但并不改变频道频率。每一个 DSSS 链接仅使用一个频道，不会在多个频率之间跳换。如图 1-3 所示，与常见无线电信号相比，DSSS 发射使用了较宽的带宽但功率较低。左边的数字信号是常见的发射，能量集中在较窄的带宽中。而 DSSS 信号(右边)使用了相同能量，但却把这些能量分散在一段较宽的无线电频率带中。很显然，22MHz 的 DSSS 频道要比 FHSS 系统中的 1MHz 频道宽得多。

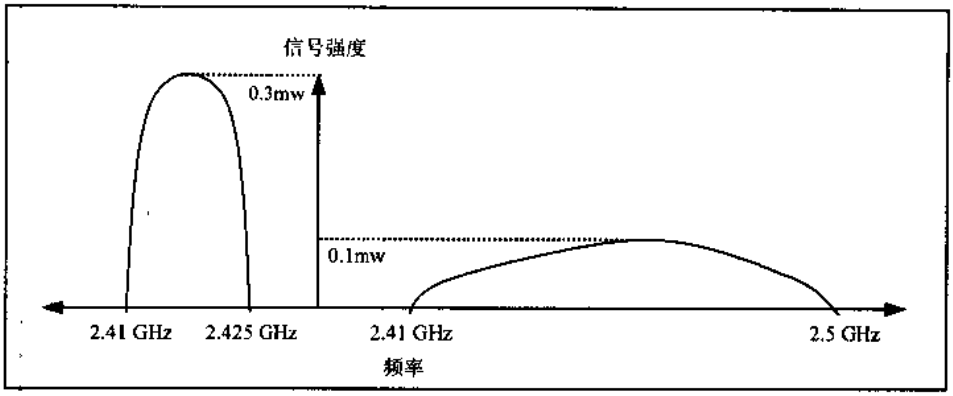

图 1-3　常见无线电信号和 DSSS 无线电信号

DSSS 发射器把原始数据流的每一位分割成一连串冗余的位模式(被称为片)，然后把它们发射到接收器，接收器重新把这些片组合成与原来一样的数据流。由于大部分干扰会占用比 DSSS 信号更窄的带宽，因为每位被分割成几个片，接收器通常可以在解码正常信号之前识别出噪声并拒绝它。

像其他网络协议一样，DSSS 无线链路在每个数据包内交换握手信息，以便接收器可以理解每个包。802.11b DSSS 网络中的标准数据传输速率为 11Mb/s，但当信号质量不能支持这个速度时，发射器和接收器使用一个动态速率交换过程来把该速率降低到 5.5Mb/s。下面这些情况都会导致传输速率下降：接收器附近有电子噪声源，或发射器和接收器距离较远难以维持高速传输。如果 5.5Mb/s 这个速率对链接来说还是太快而难于处理，传输速率则会降到 2Mb/s，甚至 1Mb/s 以下。

1.1.3　频率分配

根据国际上的协议，在 2.4GHz 附近的这段无线电频谱可保留用于无须许可的工业、科学和医学服务中，也包括扩频无线数据网络。无须许可的 2.4GHz 扩频频率分配表如表 1-1 所列。然而，世界不同地区的实际频率分配却有些细微的差别：不同国家当局都已经分配了这些略有差异的频率带。

表 1-1　无许可的 2.4GHz 扩频频率分配

地　区	频 率 带
北美	2.4000-2.4835GHz
欧洲	2.4000-2.4835GHz
法国	2.4465-2.4835GHz
西班牙	2.445-2.475GHz
日本	2.471-2.497GHz

几乎世界上其他任何一个国家都会使用这些频带之一。频率分配上的细小差别其实并不重要(除非您想跨国(比如法国和西班牙之间)发射信号)，因为大多数网络都完全工作在一个国家或地区，并且普通信号通常只覆盖几百英尺而已。在不同国家标准之间仍存在一些重叠频带，以便保证相同的设备能在世界上任何地区合法工作。如果您要把网络适配器带到国外，您就可能必须把适配器的频道改变一下；如果一个网络在您的适配器频带范围内，那么总有一个方法能把适配器连接到网络上。

在北美地区，Wi-Fi 设备共使用 11 个频道。其他大多数国家有 13 个经过授权的频道，但日本使用 14 个频道，法国则只有 4 个频道。幸运的是，全世界都使用统一的频道编号，这样纽约地区的频道 9 则与东京或巴黎的频道 9 使用同一频率。表 1-2 列出了不同国家和地区所使用的频道。加拿大和其他一些国家跟美国使用相同的频道分配。

表 1-2　无线以太网频道分配

频　道	频率(MHz)和地区
1	2412(美国，欧洲，日本)
2	2417(美国，欧洲，日本)
3	2422(美国，欧洲，日本)
4	2427(美国，欧洲，日本)
5	2432(美国，欧洲，日本)
6	2437(美国，欧洲，日本)
7	2442(美国，欧洲，日本)
8	2447(美国，欧洲，日本)
9	2452(美国，欧洲，日本)
10	2457(美国，欧洲，法国，日本)
11	2462(美国，欧洲，法国，日本)
12	2467(欧洲，法国，日本)
13	2472(欧洲，法国，日本)
14	2484(日本)

如果不能确定其他一些国家使用哪个频道，您可以询问当地制定规章的机构，以获取特定信息。或者使用 10 和 11 频道，因为这两个频道在任何地区都合法。

注意，这些频道被分配的频率实际上都是 22MHz 频道的中心频率。因此，每个频道都会同附近频道重叠。整个 2.4GHz 带只有三个完全分开的频道的空间，所以说，如果您的网络正运行在频道 4 上，而您的邻居使用了频道 5 或 6，这样这两个网络都会把对方网络的信号当成干扰信号。这两个网络都能正常运行，但网络的性能(由数据传输

速率反映)则肯定没有相互分开的频道的网络好。

为了使这样的干扰达到最小，您可以和附近的网络管理者进行频道协商。如果可能，每个网络所使用的频道都大于等于 25MHz 或隔开六个频道号码。如果您要消除网络之间的干扰，尽量采用一个高的和一个低的频道号码。如果有三个频道，最佳方案则是频道 1、6 和 11，如图 1-4 所示。要是超过三个网络，您将不得不忍受一定的干扰，但您可以通过在已有的一对频道中间分配新频道，使干扰减到最低。

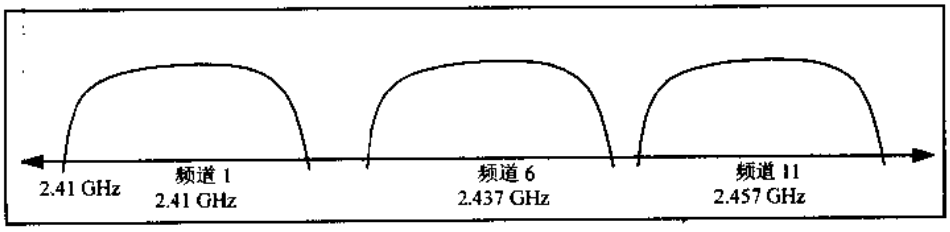

图 1-4　网络之间不会产生干扰的频道 1、6 和 11

这个问题看起来要比现实中严重。实际上，通过避开其他网络可能使用的频道，您就可使网络性能最优化，即使您和近邻使用相近的频道，您的网络也会很正常工作。除了上面的问题，您可能还会受到一些使用 2.4GHz 频带的设备的干扰，如无绳电话和微波炉。

802.11 规范和其他一些国家标准制定机构(如美国的联邦通信委员会)都对无线以太网设备可使用的发射器功率和天线增益进行了限制。其意图就是限制网络链路的传输距离，这样允许在相同的频道中存在更多不会互相干扰的网络。我们将讨论一些有关如何在这些功率限制下的工作以及扩展无线网络范围而不触犯本书后面介绍的法律的方法。

1.2　传输数据

假设现在有一堆无线电发射器和接收器，它们在相同的频率下工作并使用同一调制方法(调制就是指无线电用来把某种内容，例如音频或数字信号，转变成无线电波的一种方法)。那么下面要做的就是使用这些无线电设备发送一些网络数据。

首先，让我们来快速回顾一下计算机数据常用的结构和网络用来在两地间传输数据的方法。您或许对此已经非常熟悉，但此处仍会用一些篇幅来介绍一下。这确实可以帮助您了解无线网络的工作原理。

1.2.1　比特和字节

您可能已经知道，计算机处理单元只可以识别两种信息状态：有向处理器输入的信号或没有输入信号。这两个状态可以描述为 1 和 0 或者是开和关，或者是传号或空号。每个 1 或 0 实例是一个比特(bit)或(二进制)位。

单一比特并没有什么实际意义，但如果把八比特组成一个串(形成一个字节)，就可以有 256 个不同组合。这些组合已足够分配给字母表内的任何字母(大小写)、0~9 十个数字、单词之间的空格符号和其他一些符号(比如一些标点符号和外文字符)。现代计算机可同时识别和处理一些 8 比特的字节。处理完后，计算机会在它的输出端使用同样的比特编码。输出端可能被连接到打印机、视频显示器或数据通信通道，甚至是其他一些设备(如闪灯)上。

我们这里所说的输入和输出其实就是构成通信回路的部分。就像计算机处理器，一个数据通道每次只能识别一个比特，而不管线上是否存在信号。

在一些较短距离的情况下，我们可以用八条分开的线组成的并行电缆来传输数据，这样就可以同时载 8 条信号(或 8 的倍数)。显然，并行连接比通过一条线一次发送一个比特的方法速度要快 8 倍，但电缆的成本显然要高出 8 倍。当您试图长距离地发送数据时，就不要使用并行电缆了。当您使用已有的通信回路，比如电话线，您将没有其他选择；您必须找到一个通过同一线路(或者是其他媒介)发送所有八个比特的方法。

解决问题的方法就是一次发送一个比特，另外还得额外加入一些比特和标识每个字节开始的停顿符号。这是一个串行的数据通信通道，因为您正一个接一个地发送比特。在这个阶段，您可以不用去考虑发送这些比特的媒介究竟是什么——它可以是线上的电脉冲，也可以是两个不同的音调，或者是闪灯，甚至是附在信鸽脚上的短信，无论是什么媒介，您都必须把计算机的输出转换为传输媒介使用的信号，然后在另一端将其转换回去。

1.2.2　错误校验

在一个完美的传输回路中，从一个终端发出的信号跟另一个终端识别出的信号应完全相同。但在实际情况中，总会存在一些干扰原始信号的噪声。噪声就是所有附加到原始信号的任何信号，雷击、其他通信通道或回路的某个电接触上的污点(或者是受到鹰攻击的信鸽)都会产生噪声。不管噪声的来源是什么，它都会对数据流产生干扰。在现代通信系统里，回路中信息流通的速度是非常迅速的——每秒数兆比特，所以即使是一个很短暂的噪声都会使大量正常的比特湮没，而使您的数据变成一堆数字垃圾。

因此您就必须在数据流中包含一个叫做错误校验的过程。可以通过为每个字节添加

校验和(checksum)这样一种标准信息来进行错误校验。如果接收器发现收到的校验和不是它所期望的，它就会通知发射器将数据再发送一次。

1.2.3 信息交换

当然，要发送消息或数据流的计算机不会突然联机，然后就开始发送数据。首先它必须通知另一端的设备它已经准备就绪，然后确保预期的接收方准备接收数据。为了完成这个过程，实际的数据包含了一系列信息交换(handshaking)消息。

请求过程类似于如下内容：

源："Hey destination! I have some data for you."

目的地："Okay, Origin, go ahead. I'm ready."

源："Here comes the data."

源："Data data data data..."

源："That's the message. Did you get it?"

目的地："I got something, but it appears to be damaged."

源："Here it is again."

源："Data data data data..."

源："Did you get it that time?"

目的地："Yup, I got it. I'm ready for more data."

1.2.4 查找目的地

发生在源和目的地之间的直接物理连接上的通信不必包含任何地址或路由消息作为该消息的一部分。首先您必须建立连接(通过电话呼叫或者在交换机上插入电缆)，在连接之后，连接会一直保持到您通知系统停止连接。这种连接方式比较适合声音和一些简单的数据链接，但对一个服务于多个源和目的地的复杂网络上的数字通信就不是特别有效，因为它会一直连接该回路，即使在通道内无数据传输的情况下也是这样。

另外一种方法就是把您的消息发送到一个交换中心，该中心将保存您的信息直到与目的地的链接可用。这也被叫做存储转发(store and forward)系统。如果网络的设计对系统中的数据类型或通信量较适合的话，等待时间将不会很明显。但如果通信网络覆盖了大面积地区，在到达最终目的地之前您可能会把消息发送到一个或多个中间站。这种方法的好处就是大量消息可以在发送时共享同一回路。

为提高网络效率，您可以把超过一些假定限制长度的消息分成一些片断(又叫包)。来自多个消息的包可以在同一回路里传输，在交换中心之间传输时可能包含一些来自

其他消息的数据包，在目的地把它们重新组合到原始消息中。每个数据包还应该包含另外一组信息：包的目的地地址、在原始发射器中相对于其他数据包的序列顺序等。其中一些信息用于指示交换中心将每个包转发到何处，而其他信息告诉目的地设备如何将包中的数据重新组织成原始消息。

每次在往通信系统里添加另一活动层时，会重复同一模式。每层都会向原始消息添加额外信息，然后在完成这条信息要求它做的工作后将它自动删除。在一条消息从无线网络上的一台笔记本电脑，通过公司 LAN 和 Internt 网关传输到连接到另一 LAN 上的远程计算机上后，在接收方读取原始消息之前会有大量消息附件被添加或删除。帧指的就是一个数据包，它在包含消息内容的位前包括了地址和控制信息，后面还附加了一个错误校验序列。有线和无线网络都将数据流分成帧，帧中包含了各种信息交换消息以及原始数据。

通过一个复杂投递系统，将比特、字节、包和帧看作投递的数字形式的信件，可帮助理解这些概念：

(1) 写好一封信，然后把它装进信封。在信封上写上收信人的地址。

(2) 把信送到信件处理间，那儿会有一个职员负责把您的信放进大一点的特快信封里。大信封上写上收信人所在公司的名称和地址。

(3) 职员把大信封带到邮局，会有另一个职员把它放到邮寄袋里。邮局会在袋子上贴一个标签，上面注明了收信人公司所在邮局位置。

(4) 袋子被装到开往飞机场的某卡车里，在那里会跟其他一些同样发到这一目的城市的袋子装到集装箱里。集装箱上面贴有告诉货物搬运工此集装箱内装有邮件的标签。

(5) 货物搬运工把集装箱放到飞机上。

(6) 现在，您的信先是被放到信封里，接着信封被放到特快的大信封，大信封又被装进邮件袋，然后邮件袋又被放入集装箱，最后集装箱被装上飞机。飞机接着飞到目的地城市附近的飞机场。

(7) 在目的地的飞机场，地勤人员把集装箱从飞机上卸下来。

(8) 货物搬运工从集装箱中搬出邮件袋，把它放到另一个卡车里。

(9) 卡车把邮件袋送到收信人公司附近的邮局。

(10) 在邮局里，另外有职员把大信封从邮件袋里取出，然后把它交给邮递员。

(11) 邮递员负责把特快专递的大信封送到收信人公司。

(12) 收信人公司的传达员从大信封中取出信件，并把它交给最终的收信人。

(13) 收信人打开信封并阅读信件。

在上面的每个步骤中，包裹外的信息总会告诉某人应该如何处理它，但这个人不用去管包裹里面究竟是什么。无论是您还是最终看到信的人都没有看到特快专递的信封、邮件袋、卡车、装运箱、飞机，但上面的这些包裹在您的邮件传递过程中都起到非常

重要的作用。

电子消息不需要这些信封、袋子、装运箱，而是用数据串来告诉系统该如何处理消息并送往何地，但最终的结果仍是您的消息。在 OSI 网络模型中，每个传输模式都是一个独立层。

幸运的是，网络软件会自动添加和删除消息的前导信息、地址、校验和和其他一些信息，这样您和您消息的接收方就绝不会看到这些附加信息。但是，添加到原始数据上的每一项都会加大数据包或帧的大小，因此这也增加了通过网络传输数据所需的时间。由于理论数据传输速度包括了开销信息和“实际”数据，所以无线网络中的实际数据传输速度会慢许多。换句话说，即使网络速度能达到 11Mb/s，实际文件传输速度也可能只有 6 Mb/s 或 7Mb/s。

1.3　802.11b 无线网络控制

802.11b 规范控制着数据在物理层(无线电链路)中传输的方式，另外它还定义了 MAC(媒体访问控制)层来处理物理层和其他网络结构之间的接口。

1.3.1　物理层

在 802.11b 网络中，无线电发射器会在每个包前添加一个 144 位的前导，包括接收器用来与发射器保持同步的 128 位信息和 16 位的帧起始字段。接着是 48 位头信息，包含了数据传输速率、包内数据长度和错误校验序列的信息。这个头信息也被称作 PHY 前导，因为它控制着通信链路的物理层。

由于在头信息里规定了数据所能传输的速率，通常前导和头信息的传输速率都只能是 1Mb/s。因此，即使您的网络速度能在 11Mb/s 下工作，有效数据传输速率也会相当慢。实际上，您所能期望的最快速率也只能在平常速率的 85%以下。当然，数据包中其他类型的开销也降低了实际速度。

144 位的前导是从一些旧且慢的 DSSS 系统继承而来，之所以在规范里仍然保持了这段信息，是为了确保 802.11b 设备能与以前的标准兼容，但实际上，它已不起任何作用。因此，规范提供了另外一个仅有 72 位前导的选择。在这个较短的前导中，同步字段中有 56 位，以及用于长前导中的相同的 16 位帧起始域。这个 72 位的前导与以前的 802.11 硬件不兼容，但只要网络上的所有节点能识别这个短前导格式，这也就无所谓。从其他一些方面考虑，短前导和长前导一样好。

网络处理一个长前导最多要花 192ms，而处理短前导则可能只要 96ms。换句话说，使用短前导会削减在每个数据包上花费的一半开销。这对于实际数据吞吐来说有很大

的不同，特别是音频流和视频流、Internet 音频服务等。

一些厂家默认使用长前导，而其他则使用短前导。通常可以在网络适配器和接入点的配置软件里修改这些前导长度。

对大多数用户来说，只要前导长度对于网络中的所有设备都一样，就不需要了解这项技术细节。10 年以前，用电话和调制解调器来把计算机连接到网络上是最常见的方法，这时我们总是担心通过调制解调器呼叫时该怎样设置“数据位”和“停止位”。您可能从来不用知道停止位究竟是什么(停止位其实是指老的机械式电传打印机在发送和接收每个字节后返回到闲置状态所需的一段时间)，但您可能知道每次结束的停止位必定会是一样的。前导长度其实也是同样的模糊设置：网络中的每个节点的前导长度必定都一样，但大多数人都不用知道或关心它究竟指的是什么。

1.3.2 MAC 层

MAC 层控制通过无线电网络的通信量。它通过一组名为载波监听多路访问/冲突检测(CSMA/CA，Carrier Sense Multiple Access with Collision Avoidance)的规则，防止数据发生冲突，它还支持 802.11b 标准中指定的一些安全功能。当网络中有不止一个接入点时，MAC 层会将每个网络客户端与提供最好信号质量的接入点相关联。

如果网络中有多个节点试图同时发送数据，则 CSMA/CA 会命令发生冲突的一个节点取消发送并等待一段时间，然后让幸存的那个节点发送它的数据包。CSMA/CA 的工作方式如下。当网络中一个节点准备发送数据包时，它先监听一下是否有其他信号。如果不存在其他信号，则会等待一段随机(很短)时间并再次监听一下。如果还没有其他信号，节点就会发送这个信号。接收这个数据包的设备对这个数据包进行评估，如果数据包是完整的，就会返回一个确认信息。如果发送的节点没有收到这个确认信息，它就会假定网络上发生了跟其他数据包的冲突，从而会等待另一段随机时间，然后重新再试。

CSMA/CA 还有一个可选特性，它可以设置接入点(连接无线 LAN 和主干网的桥)作为一个点协调器，通过这个点协调器可以对试图发送时间关键数据类型(如音频或流媒体)的网络节点设置优先级别。

MAC 层有两种确定网络设备已授权连接网络的验证方法：开放式验证和共享密钥验证。当您配置网络时，网络上所有的节点都必须使用同一种验证方式。

在允许其他更高层发送数据之前，网络通过交换(或试图交换)一些控制帧来支持 MAC 层的所有功能。另外它还在网络适配器上设置下述一些选项：

- **电源模式**　网络适配器支持两种电源模式：CAM(Continuous Aware Mode，持续识别模式)和 PSPM(Power Save Polling Mode，节电轮涡模式)。在 CAM 中，无线电接收器始终开启并消耗电量。在 PSPM 中，接收器大部分时间是闲置的，

但它会周期性地接受接入点传来的新消息。顾名思义，PSPM 可以为诸如笔记本和 PDA 等移动设备节省电池电量的消耗。

- **访问控制**　网络适配器拥有拒绝未授权用户访问网络的控制能力。802.11b 网络使用两种访问控制方式：SSID(网络名称)和 MAC(标识每个网络节点的惟一字符串)。每个网络节点必须置入 SSID 信息，否则接入点无法与该节点发生联系。可选的 MAC 地址表可用来将访问局限于其地址在列表中的无线电。
- **WEP 加密**　网络适配器还控制着 WEP(Wired Equivalent Privacy，有线等同隐私)加密功能。网络使用 64 位或 128 位加密密钥对无线电链路中传输的数据进行加密或解密。

1.3.3　其他控制层

802.11 标准中规定的所有活动均发生在物理层和 MAC 层。更高级别的一些层则控制着寻址和路由、数据完整性、语法和包含在数据包里的数据格式等信息。无论通过什么媒介(电缆、光纤或无线电链路)传输数据，这对于高层来说并不会有多少差别。因此，您可以和任何一种 LAN 或其他网络协议一起使用 802.11b 网络。同样的无线电也可以处理 TCP/IP、Novell NetWare 或者其他一些内置到 Windows、Unix、Mac OS 等操作系统中的所有其他网络协议。

1.4　网络设备

一旦定义好无线电链路和数据格式，下一步就是建立一个网络结构。计算机如何利用无线电和这样的数据格式来实际地交换数据呢？

802.11b 网络包含两类无线电：站和接入点。站可以是一台计算机或其他如打印机这样的设备，它通过内置或外置无线网络接口适配器连接到无线网络。接入点是无线网络的基站，也是把无线网络和传统有线网络连接起来的桥梁。

1.4.1　网络适配器

用于站上的网络适配器可以采用下列一些物理形式：

- 适合于大部分笔记本电脑的 PCMCIA 插槽的插入式 PC 卡

为了绕过计算机内部的屏蔽，大多数无线 PC 卡适配器中的天线和状态灯都会超出卡插槽开口大约 1 英寸。其他 PC 卡适配器都会有外部天线的插口。

- 适合于台式机的 PCI 卡上内置网络适配器

大多数 PCI 适配器实际上就是 PCMCIA 插槽，用户可以把 PC 卡插到计算机后部。但有一些是直接构建于 PCI 扩展卡上的。除了后面板插槽，还可以从 Actiontec 和其他一些厂商那儿获得一些适合于计算机外部前面板扩展槽上的独立 PCMCIA 插槽。

- 外置 USB 适配器

USB 适配器通常是比 PC 卡更好的选择，因为您可以更方便地将电缆末端的适配器移至一个离最近的接入点有最佳的信号路径的位置。

- 用于笔记本电脑的内置无线适配器

内置适配器是插在计算机主板上的模块。在操作系统看来其实它与 PC 卡一样。内置无线电的天线通常隐藏在计算机的折叠式屏幕里。

- PDA 或其他手持设备的插入式适配器
- 其他设备(如 Internet 电话机和办公用或家用设备)的内置网络接口

只要这个适配器的驱动程序可用，网络适配器就可以在任何操作系统中运行。实际上，这意味着您可以找到适合于任何系统的 Windows 驱动程序，而如果您的计算机运行的是 Mac OS、Linux 或 Unix，选择就少得多。您可以在本书后面介绍操作系统的一些章节中找到适于 Linux 或 Unix 的驱动程序。

1.4.2 接入点

接入点经常与其他一些网络功能结合在一起。很可能找到通过数据电缆插入到有线 LAN 中的独立接入点，但还有许多其他方法。常见的接入点配置有：

- 通过桥接到以太网端口而连接到 LAN 的基站。
- 包括带有一个或多个有线以太网端口以及无线接入点的交换机、集线器或路由器的基站。
- 提供连接电缆调制解调器或 DSL 端口和无线接入点的网桥的宽带路由器。
- 将一个无线网络接口适配器用作基站的软件接入点。
- 支持有限个操作频道的住宅网关。

各个厂家的接入点的外观设计(如图 1-5 所示)都不一样。有一些是可以安装在远离视线的地板或墙上的工业设备，而另一些则采用流线式设计，似乎特别用于咖啡桌上。有的接入点有内置天线，有的带有垂直的短天线，还有的则留有用于外接天线(可能和无线接入点一起提供)的连接器。不管它的外观和大小如何，每个接入点都会有一个用来发送和接收网络站之间消息和数据的无线电，以及连接到有线网络的以太网端口。

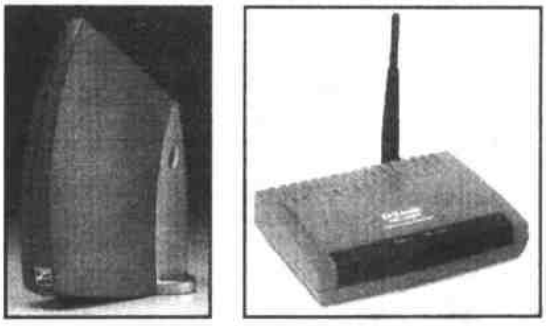

图 1-5　来自 Zoom 和 D-Link 两家公司的接入点

1.4.3　工作模式

802.11b 网络有两种工作模式：特别(ad hoc)网络和基础(infrastructure)网络。顾名思义，特殊网络通常是暂时性的。一个特殊网络通常都是自包含的站组，无须连接到更大的 LAN 或 Internet 上。它包含两个或更多无线工作站，不存在任何接入点，也不连接到外界其他设备。特殊网络又可以叫做对等网络和 IBSS(Independent Basic Service Sets，独立基本服务集)。图 1-6 所示是一个简单的特殊网络。

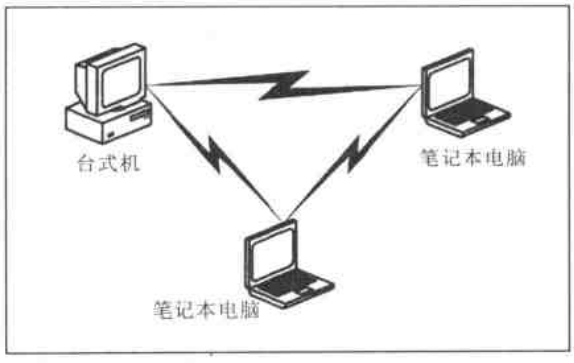

图 1-6　有三个工作站的特别无线网络

基础网络有一个或多个接入点，通常都连接到一个有线网络上。各无线站通过接入点交换信息和数据，接入点把这些信息转发到无线网络的其他节点或有线 LAN 上。任何需要通过接入点有线连接到打印机、文件服务器或 Internet 网关的网络都是基础网络。图 1-7 显示一个基础网络。

仅有一个基站的基础网络也叫基本服务集(Basic Service Set，BSS)。当一个无线网络使用两个或两个以上的接入点时，网络结构就变成了扩展服务集(Extended Service Set，ESS)。还记得前面提到的一个叫做 SSID 的网络 ID 的技术术语吗？可将仅有一个接入点的网络叫做 BSSID，而将两个或多个接入点的网络叫做 ESSID。

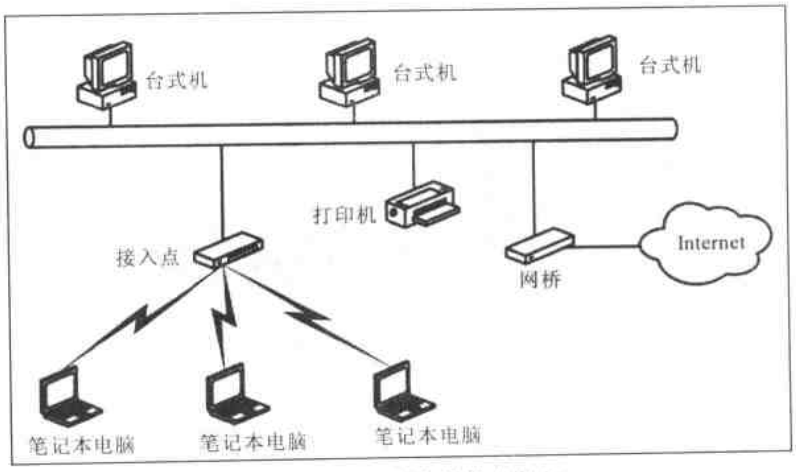

图 1-7　一个简单的基础网络

有多个接入点的网络(扩展服务集)会产生一些新的复杂问题。首先，网络必须有一个只让一个基站来处理来自特殊站的数据的方法，即使这个站在多个基站范围内。此外，如果这个站在网络会话中移动，或者某个本地干扰突然出现在第一个接入点的附近，则网络可能必须将连接从一个接入点移交给另一接入点。802.11b 网络处理这一问题的方式如下，每次只会将基站同一个接入点相关联，而忽略掉那些不相关联的站的信号。当信号在某个接入点衰减而在其他接入点里得到增强，或者是网络通信量迫使网络重新平衡负载时，网络会重新把该站与一个能提供合适服务的新的接入点相关联。如果您觉得这很像蜂窝电话系统处理漫游的方式，那么您是完全正确的；甚至术语也一样——也叫漫游。

1.5　小结

无线电链路、数据结构和网络体系结构是构成 802.11b 无线以太网络内部装置的三个重要部分。像大部分其他网络的组件一样(大多数管线系统)，这些元素对使用网络的用户来说是透明的——如果用户能收发信息、读取文件以及在网络上执行其他活动，他们都不用担心这些底层的细节。

当然，这是假定网络总是能像预期的那样工作，且没有用户拨打网络求助电话询问为何他们不能看到邮件。现在您已经阅读完本章，您或许能比那些 95%使用 Wi-Fi 网络的人要清楚，您的无线网络是如何使消息在异地之间传送的，而且在客户服务人员告诉您要使用 11 频道，或您必须调节前导信息长度，又或您的适配器是在基础网络中运行等内容时，您能清楚地知道他在说什么。

第2章　实现无线所需的设备

无线本地网络(LAN)要求一些不同于传统有线网络的硬件设备。显然，最大的不同就是在网络服务器和无线客户计算机和其他一些构成网络的设备间不存在电缆线，但这不是惟一不同之处。Wi-Fi 网络必须有无线电收发器来作为连接网络和网络上有线和无线部分的接口。

本章将讲一下组成无线网络所需要的部件，另外还提供了一些建议，说明能满足特定需求的最佳部件。在您阅读接入点、网络适配器、天线的不同特点和功能的描述时，请记住无线网络设备的市场竞争是非常激烈的，而且它更新很快。如果一个厂家能提供很多具有新功能的接入点或适配器，在几个月后您一定可以看到其他竞争厂家也出了同样特点的产品。因此，这一章并不会谈到哪个特殊的牌子或产品；在您阅读完本章后，任何这样的推荐都会显得过时了。

2.1　大部分部件是一致的

在谈及网络的特点和功能时，有必要了解一下在网络中使用不同厂家的 802.11b 设备时的一些规则和实际状况。可以做到这一点，但肯定不会如 Wi-Fi 联盟所声称的那么容易。

多家公司生产符合 Wi-Fi 认证的设备。为获得认证，每台设备都必须在 Wi-Fi 联盟的独立测试实验室上通过协作性测试。如果一个接入点或网络适配器附有 Wi-Fi 标志，就表示它已经通过了和一些先前获得认证的其他供应商的硬件之间的扩展性测试。

来自不同厂家的接入点和网络适配器外表上可能很不相同，每个厂家都会对自己的产品出一套配置软件，但内部的无线电回路其实都大致相同。市场上有很多品牌的网络适配器，其实都是在和公司之间的合同下生产的，几乎每个人都使用来自一些标准芯片组的产品。

换句话说，在同一个网络里使用通过 Wi-Fi 认证的接入点和适配器的任意组合是可能的。不过这只是可能。在一些精心运作的测试里，熟悉 802.11b 网络内部工作原理的一组技术人员可以在很严谨的实验室条件下，把由不同厂家的产品构成的网络正常运行起来。

这是不是意味着从没有安装过无线网络的一个户内人员或小公司的 IT 职员也能把这些产品组合起来工作呢？哦，或许可以做到，但也可能在第一步测试时便告失败。

要把所有配置选项都设置为正确值要花很多时间和精力。其实来自不同厂家的产品一般都会有不同的默认设置。例如，有些系统默认使用短前导(preamble)，有的则是用长前导。有些设置要求 ASCII 码组成的 WEP 密钥，有的则要求是十六进制的密钥。您可以使这些部件共同工作，但这可能是一件痛苦的事情。

一般来说，使用来自一个厂家的硬件配置网络可能会很容易，但有时候，这无法实现，也不是最佳选择。您可以控制网络中接入点的品牌，也可以在桌面计算机上使用同一品牌的适配器，但或许会有一个网络用户使用一个您未曾听说的品牌的 Wi-Fi 适配器，他要求您把他的计算机也连接到网络上。或许这个适配器买自旧货市场，或许是一台崭新的掌上计算机内的配件，也可能是您的女儿学校里所要求的校园网所使用的适配器。这样或那样的原因都会让您不得不把来自不同厂家的硬件和软件整合进同一网络里。

本书会帮助您理解如何所所有组件共同工作。在配置第一批硬件时，通过使用同一个厂家的设备，可减少麻烦。

2.2　网络适配器

网络适配器是计算机和网络之间的接口。在无线网络中，适配器包括一个能从计算机发送数据到网络的无线电发射器，和一个能检测包含网络数据的传入无线电信号的接收器，通过接收器把信号传送到计算机内。对于操作系统来说，无线适配器其实与其他网络接口是一样的。

在选择接口适配器时得要考虑到以下几点：物理包、天线型号(内置或外置)、与网络接入点和其他网络节点的兼容性以及与操作系统的兼容性。当然，还要考虑选用计算机硬件或软件的所有标准：易用性、技术支持能力和其他用户对该产品和厂家的满意程度等。

2.2.1　外形因素

多数情况下，无线适配器插入一种计算机高速 I/O 端口：内部扩展卡槽、PCMCIA 插槽或 USB 端口。最新的笔记本电脑例外，它包括可选内置 802.11b 接口，该接口使用内部扩展槽，如微 PCI 或 Apple AirPort 或安装在主板上。PDA 所用的网络适配器通常都适合于 CompactFlash 插槽。

每种型号的适配器都有其优缺点。特殊包的选择取决于您所将和适配器使用的计算机和您的个人喜好。例如，如果您想把笔记本电脑连接到网络上，PC 卡通常是最好的选择，因为它不占用很多空间而且易于安装，也不会强制您使用一个特制的电缆。但

在台式系统中，最好使用内置扩展卡上的接口适配器或 USB 适配器。

1. PC 板卡

PC 板卡上的适配器是最为流行的，因为大多数无线以太网络都是用于把笔记本电脑连接到已有的 LAN 上。几乎每个 802.11b 设备的生产厂家都至少有一条 PC 卡适配器的生产线。

PC 卡上的无线适配器较紧凑，它不会太增加便携式计算机的重量，这也是它最大的优点。然而要注意的是，当您不需要网络链接时，一定要从计算机中取出适配器，否则适配器仍会不停地发射一些多余信号，这可能会使入侵者不经允许就侵入您的计算机。大多数 PC 卡适配器都有节电功能，但即使它被终止运行，仍会不必要地消耗计算机电池的少量电量。

如果您把计算机带到一个商业客机上，拔出适配器就显得尤为重要了。和移动电话或其他无线电一样，航空公司是不允许在飞机上使用无线网络的，这是因为这些设备会对飞机导航系统产生干扰。

由于都必须适合于计算机的 PCMCIA 插槽，所以 PC 卡适配器的外观几乎都一样。如图 2-1 所示，大小跟信用卡差不多，一端是连接器，另一端是内置天线的塑料封套或是外置天线的连接器。

图 2-1　Xircom 公司的天线以太网络适配器(带有内置天线)

大多数 PC 卡适配器在超出 PCMCIA 插槽末端的部分都会有一到两个显示灯。其中的一个灯在适配器接通计算机的电源时会亮，另一个灯在适配器检测到来自于接入点或特别网络中其他节点的活动无线电链接时会亮。

很多 PC 卡适配器对于不同系统采用两根内置天线，因为系统会不断比较从两条天线所接收到的信号的质量，然后自动选择信号强的那一条。尽管 PC 卡中两条天线仅有 1-2 英寸，但性能确定比一条天线要好。

PC 卡上的适配器通常会有不同的内置全向天线，但有些厂家也提供用于外置天线的连接器。选择内置天线还是外置天线总要作一下权衡。多数情况下，内置天线和便携式计算机一起使用要方便的多，因为它不要求携带一根单独的天线和电缆线。但我

们可以更容易地在电缆末端调整天线的确切位置，而不必试图将计算机的侧边或是后部放到某个接收性能好的位置，从而可以舒适地看到屏幕并使用键盘。如果您想链接到处于网络覆盖区域边缘的接入点时，或者您正在一个有很多干扰的位置中工作，一个独立的高增益定向天线会比大部分 PC 卡的内置天线有更好、更可靠的网络性能。

2. USB 适配器

如果您的计算机上有 USB(通用串行总线，universal serial bus，大多数 1999 年后出厂的台式机和笔记本都有)端口，无线 USB 适配器是把计算机连接到 802.11b 网络的最好方法。适配器通过一根电缆连接到计算机，因此将整个适配器(连同内置天线)移到一个能提供最好的网络性能的位置并不困难。即使最佳的位置是在书柜或文件柜的顶上、计算机桌下的地板上，适配器的位置都不会对使用计算机带来影响。由于不用拆开计算机来安装 USB 设备，因此安装 USB 适配器要比内置扩展卡上的适配器要方便的多。

USB 适配器有很多种外形和大小，也反映了生产厂商的设计理念。绝大多数 USB 适配器的天线都是固定的，经常被放在合页或转动枢轴位置，允许用户对他们的位置作最佳调整。因为 USB 适配器的天线较 PC 卡适配器的大且易于操作，通过 USB 适配器一般都能接收到较好的信号(但请记住您不能期望速度上能有什么提高)。

图 2-2 所示是一个来自 D-Link 的 USB 无线适配器。就像 PC 卡适配器一样，大部分 USB 适配器也从计算机上连接电源，因此它们不需要用一个独立的电池或外部电源。

图 2-2　USB 无线适配器是通过电缆连接到计算机的独立设备

3. 内置扩展卡

最常见的内置无线适配器都是那种装在 PCMCIA 插槽内的 PC 卡，而这些插槽都是适合 PCI 或 ISA 的扩展槽。适配器可以插在计算机后面安装板上某个槽中。这也给那些生产厂家带来不少便利：他们可以将他们单独出售的同样的 PC 卡适配器用于便携式计算机中，然后组合第三方的插槽并重贴上标签，PC 卡的金属外壳有效屏蔽了无线电信号对计算机内部的干扰。

没有什么比在计算机内部放置无线适配器的天线更糟糕的地方了。如果适配器有内置天线，您可能无法很容易地为提高信号质量而改变天线位置。这个卡从计算机壳后伸出，在那儿您就不能看到指示灯。绝大多数桌面计算机后面会有很多电缆线和连接

器，这些都会对无线电的发射形式产生影响。而计算机后面的金属底板则会成为适配器和较近的接入点之间的阻碍或多路径干扰源。

当然，PCI 或 ISA 卡适配器完全可能正确工作；请不要认为它是在您已经尝试在您的网络里使用它时才能工作。

如果您遇到麻烦，可以有很多解决方法。如果计算机上有 USB 端口，显然您可以选择无线 USB 适配器。如果在计算机外边没有 USB 端口，您或许可在主板上找到一个 USB 端口；如果是这样，用一根不是很贵的电缆和支架就可以把端口拖到计算机底板上。对于没有 USB 端口的老主板来说，PCI 或 ISA 扩展槽上的插件 USB 端口是一个选择。

如果不能选择 USB 适配器，试试内置适配器也行。尽管它有很多缺点，但它可以在大多数情况下平稳地工作。

如果问题出在信号质量上，请换一个带有外置天线连接器的适配器，因为它要比内置天线的适配器性能要好。Cisco、Orinoco、Zoom 等厂家都生产带有外置天线连接器的适配器。

您或许还想在您的 PC 卡适配器上安装一个卡读取器，它可以装在台式或塔式计算机前面的多余外部扩展槽中。这使适配器要比把它放置在后面方便得多，而且也避免和计算机后面那一堆电线和插头混在一起。

4. 内置适配器

一些主要品牌的笔记本电脑已开始将内置 802.11b 网络接口适配器作为可选功能。这些计算机有一个直接安装在主板上的模块，天线则在也控制屏幕显示的蚌壳部分中。

使用内置适配器最明显的优点就是用户不必再为计算机携带一个附件(可能会遗忘或丢失)。如果有缺点的话，那就是在修或更换旧计算机时不能把它拆下来用到别的计算机上。如果备份单元没有内置适配器(也有可能，因为它或许比原先的计算机老)，用户或网管则需要提供一个新的 PC 卡适配器或干脆不用这台计算机联网。

内置无线适配器在下一代便携式计算机中将变得很平常。要获得更方便的配置，花费也就和那些 PC 卡适配器差不多。这并不是说就要把您的计算机更换成有内置无线适配器的新式计算机，但如果您想添置一台新计算机的话，这是值得添加的一项功能。

如果您正在使用内置无线适配器，那么要确保有一个方法能在您不使用它时能方便地禁用它。否则，它的无线电部分会消耗比必要时多的电量，而且它产生的无线电信号会对其他使用相同的无许可的 2.4GHz 频率的用户产生干扰。

2.2.2　内置与外置天线的比较

多数接入点和绝大多数无线适配器都有固定的全向天线。对大多数用户来说，在许多情况下，这些内置天线将会在接入点和附近计算机间发送和接收强大的、完整的数

据流。但如果因为距离、阻碍物、其他无线电信号的干扰等原因，带有内置天线的适配器没有提供足够好的信号，解决问题的最好方法就是使用外置天线。单凭经验来看，使用外置天线能提供的信号要比内置到 PC 卡适配器上的天线至少增强 15%。

如果您确定了您的网络覆盖地区存在盲点，对于该区域的网络节点(例如不同位置的桌面计算机)来说，带有外置天线连接器的网络适配器(而不是内置天线)可能是好的选择，但在您登录到网络之前安装一根单独的天线似乎更麻烦，因此带有内置天线的 PC 卡是笔记本电脑和其他便携式设备的最好选择。

记住，在基站和无线网络适配器之间的链接中有两根天线——一端一根。每个终端的高增益天线都会对链接产生影响，因此替换接入点或网络接口上的标准天线则同等有效。然而，一根定向天线会把大部分信号集中在某个方向上，因此一个定向接入点天线会降低对其他网络节点的链接质量，如图 2-3 所示。

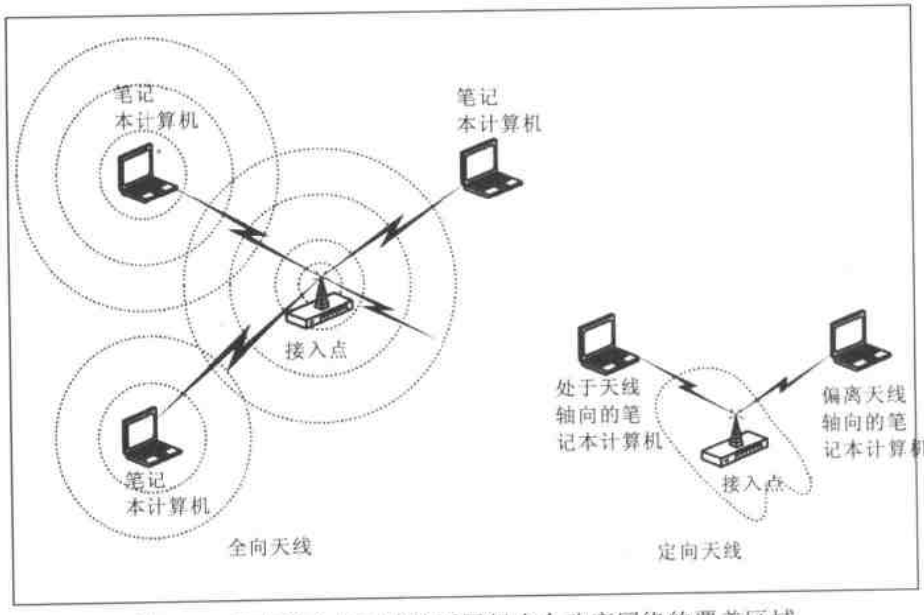

图 2-3　定向和全向天线的不同组合会改变网络的覆盖区域

您可以在本章后面的“外置天线”一节中了解到更多关于外置天线的细节。

2.2.3　互操作性

Wi-Fi 认证被用来确保来自不同厂家的接入点和无线适配器能无缝地协作工作，但其实还有一些特点和配置选项，使得在这些硬件的特定组合间交换数据很困难或不可能。例如，有些设备需要 128 位的加密密钥，而其他设备仅支持 64 位密钥。如果接入点需要 128 位的验证，那么短的密钥就不行了。

避免这种情况发生的简单方法就是从同一个厂家购置硬件，并确保使用的不是不兼

容的产品(例如同是来自 Orinoco 公司的网卡，一个使用 64 位密钥，一个使用 128 位 WEP 密钥)。另外，只要购置新的产品，就要连同网络其他部分测试每个新组件类型，如果不能兼容，最好将该情况告知您的产品供应商。

2.2.4　操作系统兼容性

就像计算机上的其他外围设备一样，无线网络适配器要求特定的驱动程序，程序中包括允许适配器和计算机中心处理器之间交换数据的控件和接口。您可以确定和适配器提供的软件盘里有 Microsoft Windows 的驱动程序，但如果您想链接到使用 Unix 或 Linux 的计算机，这就没有任何好处。如果您使用的是 Macintosh 系统，Apple 公司的 AirPort 适配器或者类似的 Orinboco 适配器则可能是最佳选择。

如果您的网络适配器没有附带合适的驱动程序，那您可能不得不去其他地方寻找或者选择另外一个支持您的操作系统的适配器。寻找驱动程序的最佳去处是生产厂家自己的技术支持 Web 站点，在那里可能会有大量可免费下载的驱动程序。如果您在那儿也找不到，就向厂家的技术支持中心发一个需求信息；他们或许会知道支持您的操作系统的第三方软件，或许还会邀请您参加尚未发布的一个新驱动程序测试。

如果厂家不能帮助您，请千万不要放弃。大多数适配器都有相近的内部回路，因此也有可能使用一个其他品牌的适配器的驱动程序。例如，Xircom CWE1100 适配器使用和类似的 Cisco 适配器相同的驱动程序。您还可以阅读第 8 和 9 章，从用户组和在线文档中查找 Linux 和 Unix 的驱动程序的其他来源。

如果没有驱动程序，您的适配器几乎毫无用处。如果实在找不到适合您的操作系统的驱动程序，就只得更换一个适配器了。

2.2.5　易用性

每个无线适配器都有一个配置实用程序来对操作模式、频道号和所有其他配置选项进行控制，这些配置必须和同一网络上的其他节点的设置匹配。生产厂家通常在销售适配器时附有配置程序的驱动光盘或软盘，但您还可以在它们的网站上找到更新版本的驱动程序。

每个配置程序都会以不同方式组织可选设置和状态信息显示。有些使用一个单独窗口，所有的选项在一个地方，而其他则会将信息分成几个单独部分。有些用数字形式显示信号的强度和质量，而有的则用图形方式显示。图 2-4 和 2-5 给出了两种表示相同信息的不同方式。

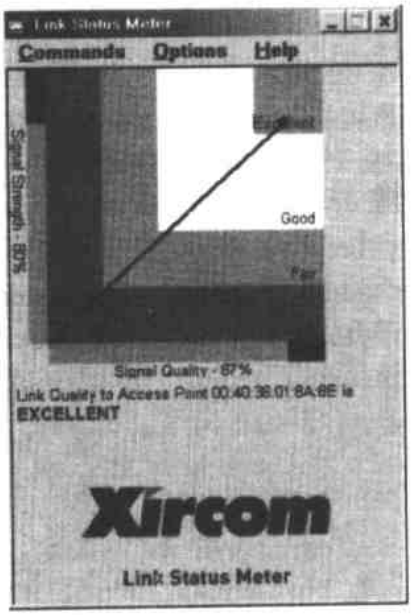

图 2-4　Xircom 的 Link Status Meter 用图形方式显示信号强度和质量，Cisco 公司使用类似工具

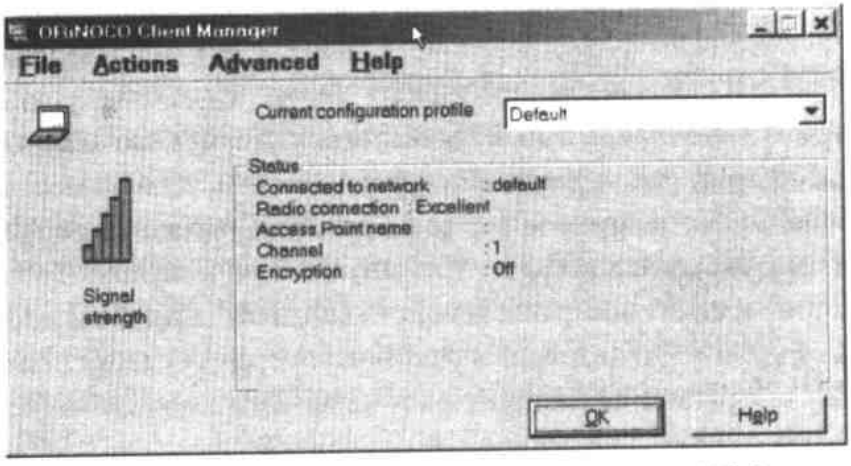

图 2-5　Orinoco Client Manager 用文本方式显示当前网络状态

理想状况下，日常用户不必考虑这些配置实用程序。但如果这个用户移至一个地方或要登录到另一个网络，配置设置和选项就突然变得很重要了。遗憾的是，现在配置一个无线网络连接和以往通过电话调制解调器进行数据链接一样非常复杂。在那时，每次呼叫都要担心怎样去设置“停止位”和“终端模拟”这样的内容。现在，无线网络用户则不得不去处理诸如“前导”等虽模糊但很重要的信息。

因此，配置实用程序和状态显示必须易于明白和使用。它们都包含相同的信息和可选项，因此，选择要涉及到主观评价：您是否能看到配置窗口且明白如何改变这些设置？您是否能通过状态显示能一眼看出是否连接到网络上？就像一个著名的漫画家在

谈到一个很久以前的选举一样，“您花了钱，就应该有自己的选择。”

2.2.6　安全性

802.11b 规范包含一个叫做 WEP 的安全模式，它使用 64 或 128 位的加密密钥。64 位加密格式是通用标准，但不同厂家提供的 128 位加密技术有一些不同。因此，当增强的安全功能都处于活动状态时，不同品牌的适配器和接入点就不可能进行数据交换了。

如果增强的安全性对于网络来说很重要，最好标准化为使用一种品牌的硬件或是一组使用同样的 128 位加密的产品(例如 Cisco、Xircom、Orinoco 和 Apple 公司的 Air Port)。

第 14 章详细探讨怎样配置和使用无线网络的安全功能。遗憾的是，WEP 加密标准漏洞百出，因此并不能有效地防止网络被未经授权的用户访问。最好的方法(特别是您的网络有多个品牌的网络配件时)就是关闭 WEP 加密，使用第 14 章里所讲到的某种安全方法。

2.2.7　文档和技术支持

每家生产和销售无线以太网硬件的公司都会对他们的用户提供一定的技术支持。然而，各家公司提供的服务质量和有效性不尽相同。如果您不能从这家公司找到您需要的信息，您可能就会转向另外一家公司。

在最低限度上，技术支持一般也要做到提供详细而正确的用户手册，是一个能回答电话或 Email 发来的问题的支持中心，一个能回答常见问题的 Web 站点和能提供免费下载最新版本的设备驱动程序、配置应用程序和状态显示软件的下载中心。

每个适配器和接入点都应该有详细的用户手册，能指导用户怎样安装、配置和使用该设备，而且要求语言简洁易懂。在您购买某一计算机设备时最好看一下用户手册；带有含糊用法说明或文本(像是由某人由口语化的 Swahili 语译过来的，而其母语又是模糊的 Gaelic 方言)的手册显然是不能接受的。

即使是曾经写出来的最棒的手册都不可能面面俱到，因此给技术支持中心打电话和发电子邮件则是一个好的解决问题的手段。如果技术支持有免费电话则更好，但它并不是很关键——您或许会为了这个产品花更多的钱在这些“免费”服务上。您或许可以在一到两分钟内现场遇到一个技术人员，或者如果您打电话时很忙，您可以把您的电话留下，以便支持中心在几小时内给您回电话。无休止的占线或者没有回答特定问题的不可理解的菜单都是不能接受的。

如果您通过电子邮件把您的问题发送出去，您可以在一小时内收到确认信息，哪怕

是自动回复的，“谢谢您的问题，我们会尽可能给您的问题一个详细的回答。”您可以在下个工作日内等到这个问题的回复。

当然，回答您问题的人应该提供解决您的问题的详细信息。错误的信息往往比没有信息更糟。

大多数计算机硬件和软件公司都会有技术支持 Web 站点，它包含了从用户那儿收集到的常见问题的答案。如果您想快速地找到答案，登录到那个站点，应该很容易找到一些解决问题的方法。该站点应该还有下载中心，在那儿可以找到该公司已出售产品的相关软件和最新驱动的拷贝，包括不再继续开发的产品。

2.2.8 名声

在您决定花钱购买一个无线适配器之前，最好了解一下其他人对这个产品的使用体验。厂家或者经销商总是很乐意向您介绍这个产品的正面优点，但您不能期望这完全客观。

您可以从本地用户组织、已发布的产品评论和网络评论这些有用资源中找到关于无线以太网设备的信息。如果只是注重于每个评论或恐怖事例并不可靠，但要是您听到很多报告说某个驱动使 Windows 崩溃或 PC 卡总是过热，您就可以对这些产品作一个明确的评价了。

Practically Networked Web 站点(http://www.practicallynetworked.com)是一个非常棒的、评价和讨论无线以太网设备的站点。

总会有一个无线网络设备提供商有很差的技术支持名声——技术人员的电话总是需要很长时间等待，电子邮件回复很慢，回答的问题总是没有什么帮助。在这样充满竞争的无线以太网设备市场，您无需忍受一家不会(或不能)提供周到服务的公司。

2.3 用于特别网络的适配器

在特别网络中，每个网络适配器通过直接链接与其他节点交换数据，并不需要作为中心节点的接入点支持。特别网络对于小型、孤立的网络或直接对等文件共享很有用。例如，在路上使用笔记本电脑、在办公室里使用台式机的用户就可以在这两者之间建立一个特别网络来传输文件。或者两个拥有笔记本电脑的用户也可以使用特别网络来共享文件。

连接两个以上网络节点而不使用接入点的特别网络远没有基础网络通用，但它也是 802.11b 规范中的一部分，几乎每个网络接口适配器和无线配置程序都提供特别网络选项。

通常任何带有 Wi-Fi 标志的网络适配器都可以在特别网络中良好地运行。有必要使网路里的每个节点都被配置为特别网络选项，而且其他选项也要相同，但直接连接到其他计算机并不比连接到接入点难。

2.4　双重功能的适配器

Wi-Fi 网络已经变得很流行，但并不是这方面惟一的无线网络技术。其他一些系统也可用，例如蓝牙技术(为计算机外围设备和附件提供很短范围的连接，如双耳式耳机和键盘)，802.11a(使用不同的一组无线电频率，提供比 802.11b 网络更高速的网络链接)。它们都能解决一组不同的问题，且都能占市场一定份额。

有些厂家宣称它们的新产品组合了 802.11b 网络适配器和其他无线服务的接口。有些可以检测和使用 802.11a(5.4GHz)和 802.11b(2.4GHz)两个网络，有些则把 802.11b 网络和蓝牙整合在一起。还有一些则可能将对无线局域网的接入与蜂窝数据或其他广域网(WAN)服务整合在一起。整合过的接入点优势是显而易见的——一个设备总比两个设备易于安装和携带，另外也提供与多个网络和服务的连接。而且由于是相同的无线电发射器和接收器处理这些服务，降低了可能的干扰。

一个理想的双重服务网络适配器可以自动监测来自范围内所有兼容网络的无线电信号，并且允许用户安装对这些网络的即时连接，而且不用去考虑网络使用的链接类型。这种组合的适配器的价格应该比只认别一种网络协议的适配器略高一点。这样完美的无线网络适配器可能会在今后几年内出现。

同时，还有一些有趣的双重功能的产品已经上市。例如，GTRAN Wireless 生产了一个与 CDMA 蜂窝数据和 Wi-Fi 网络一起工作的 PC 卡适配器。它可以在绝大多数大城市里使用蜂窝电话网络以相对较慢的速度发送和接收数据，如果用户移到一个有着更快 802.11 网络信号的区域的“热点”中，适配器可以建立一个新且更快的网络连接。

有些双重模式的产品将使用 Intersil 和 Silicon Wave 在 2002 年初提出的 Blue802 技术。Blue802 技术允许蓝牙和 802.11b 连接通过一个适配器同时运行，因此计算机可以一边是用蓝牙链接到鼠标、键盘、打印机或其他计算机，一边还可以通过 Wi-Fi 网络连接到 Internet 或 LAN 上。这个确实很重要，因为 802.11b 和蓝牙都使用相同的 2.4GHz 无线电频率，且每个服务经常会造成对别的服务的干扰。Blue802 协调了这两种无线电传输类型，最优化两者的性能。

可能还有其他大量组合设备，即使它们现在还不实用。如果业界有此需求，您或许会看到同时有带有 RJ-45 以太网连接器和无线天线的网络适配器或与 56Kb/s 调制解调器使用同样数据包的无线适配器。

在您被告知能同时享用适配器支持的两个网络服务时，您也就能接受双重模式的适

配器的额外价格。Blue802 特别吸引人，因为组合的适配器将提供更好的性能，与两个分开的设备相比干扰要少得多。但像大多数电子设备一样，这些适配器的价格过段时间就会降下来，因此如果没有什么很迫切的需求，可以不购买它。

2.5 接入点

大多数无线网络接口适配器都只执行一个功能：在计算机和网络之间交换数据。相反，接入点提供了更广泛的特性和功能。它们可以作为简单的接入点，也可以和集线器、交换机或路由器组合，与附近的计算机或其他设备有线连接。另外还有用于家庭网络的一类无线接入点，称为住宅网关(residential gateway)。

接入点的外观设计不如接口适配器重要，因为接入点不必适合于计算机的卡槽或扩展面板上。有些被嵌入到简单的长方形盒子中，而有的则采用看起来更有特色的老式包装。包的外观比内部的性能和功能要次要得多，特别是当这些接入点被放在壁橱或藏在人工天花板上时。不管它的形状，大多数无线接入点都有一些安装板、支架或其他将设备装在墙或架子上的配件。

在挑选一个接入点时，您可能还会考虑一些常见的特点。如果您的站点测试通知您需要一个高增益天线，或您想把天线放在户外或其他隔离的地方，您就应该使用那些有外置天线连接器的无线接入点，而不是那种带有固定天线的接入点。如果您想在一个高通信量的网络里同时使用多个无线电频道，包含两个无线模块的无线接入点可以取代两个分离的接入点。如果接入点的最佳位置离交流电源插座较远，选用一个能提供可选的 Power over Ethernet 或是 Active Ethernet 功能的模型。

选用适合您的网络的接入点类型的最佳方法就是看您需要怎样的连接方式。是否想添加一个对现有有线网络的无线连接？或者想提供一些新的包含无线服务的有线链接？是否想使用无线网络共享 Internet 连接？上述问题的答案会帮助您选择适合于您的网络的正确无线接入点。

2.5.1 纯粹的无线 LAN

当 LAN 上所有节点通过无线电交换数据时，无线接入点则像集线器一样作为网络的中心控制点，如图 2-6 所示。严格地说，这样的网络中的“接入点”并不能提供除了网络上其他节点以外的接入。这种无线网络组合是任何一个接入点的基本功能，因此如果您想设计的话，尽量选用简易且便宜的样式来为您的网络覆盖区域提供信号。

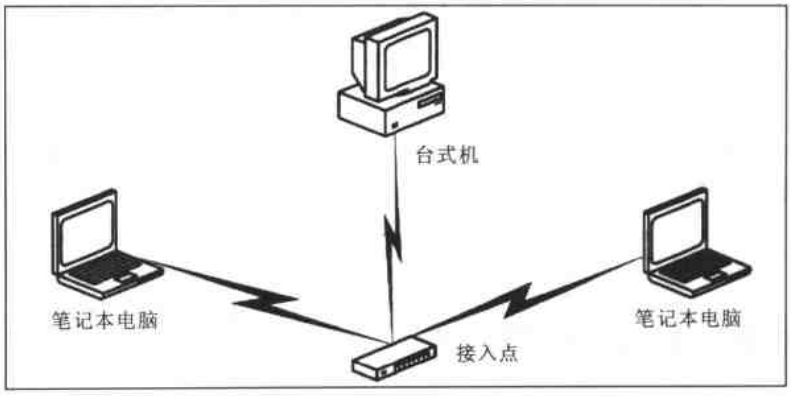

图 2-6　没有任何外部连接的简单无线网络

这种简易无线网络虽然可行，但实在没有必要在一个无线 LAN 中使用接入点。您可以在特别无线网络实现同样的工作，创建直接的点对点链接，而不需要通过中心集线器。也只有在您一开始采用无线连接，然后想把您的网络扩展成包括一个能与文件服务器、共享 Internet 连接或更多计算机和工作站的有线以太网连接，或是处于特别网络的边缘区域的计算机不能直接通信时才会考虑一个纯粹的无线基础网络(包含接入点)。

2.5.2　无线接入到有线 LAN

任何无线接入点都能作为一个基站来把无线链接添加到已有的有线网络中，如图 2-7 所示。在这里，接入点对于网络其他部分来说就像把有线节点连接到网络的辅助集线器或交换机一样。

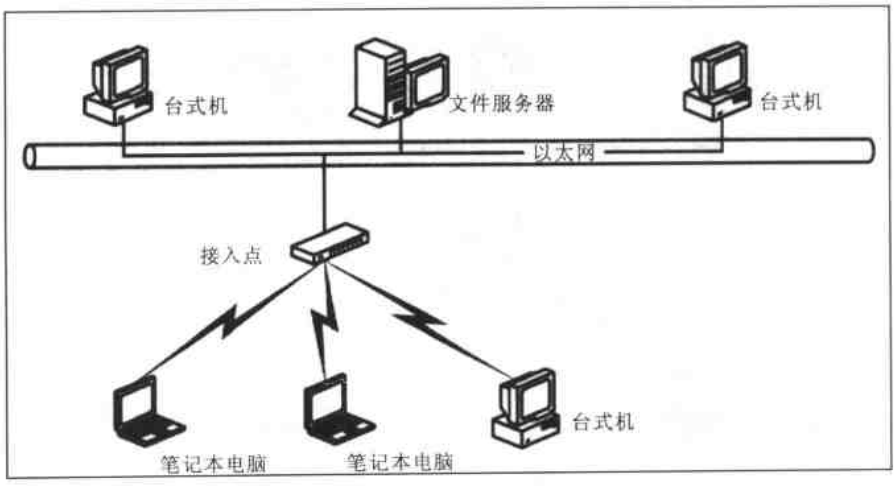

图 2-7　连接到无线以太网的无线接入点

在这种混合式的有线-无线 LAN 里，网络上的每个设备都能与其他网络节点进行数

据交换，而不用管它是怎样的连接方式。是否有一个特殊设备通过电缆线或无线电链接连接到 LAN 并不重要，因为这完全是一个无缝网络。

作为网络有线和无线部分之间的桥的无线接入点通常会有一个 10Mb/s 或 100Mb/s 的 RJ-45 以太网端口，通过这个端口可以连接一根电缆到有线 LAN 上。通常还会有另外一个作为远程终端的串行口，网管可以通过它来输入配置命令和接收状态信息。

2.5.3 组合接入点和有线集线器

在新型的包含无线连接和有线链接的 LAN 网络中，最佳的方法就是有一个能把无线接入点和有线集线器或交换机的功能组合在一起的单独设备，如图 2-8 所示。这种接入点有时也被叫作宽带路由器。

宽带路由器一般有三种网络连接：

- 无线电链接到装有无线以太网适配器的计算机
- 一到多个可以有线连接到装有网络接口卡的计算机的端口
- 宽带 WAN 端口，可以把路由器连接到主干网或把这个路由器与其他集线器或交换机相连

有些路由器还带有打印机服务器，这样可以直接把文档传到网络打印机上。

组合式接入点和集线器的最大优点就是对于家庭和小公司即便利又经济，可以很容易地用电缆把计算机连接在一起。这种组合式部件可以很快捷地把已有网络扩展至远端的有线和无线节点。

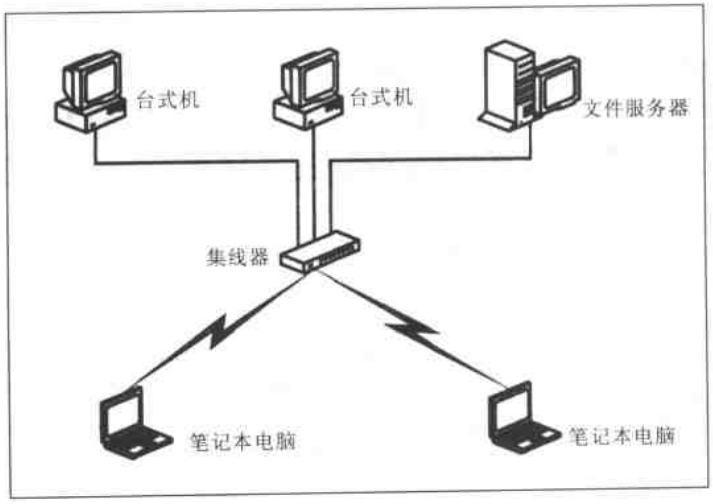

图 2-8　控制混合网络中有线和无线部分的与宽带交换机整合在一起的无线接入点

2.5.4　宽带网关

宽带网关是一个接入点，包括一个直接能连接到 DSL 或可高速访问 Internet 的电缆调制解调器的端口，如图 2-9 所示。有些网关设备有多个 RJ-45 以太网端口，通过这些端口与本地计算机进行有线连接。

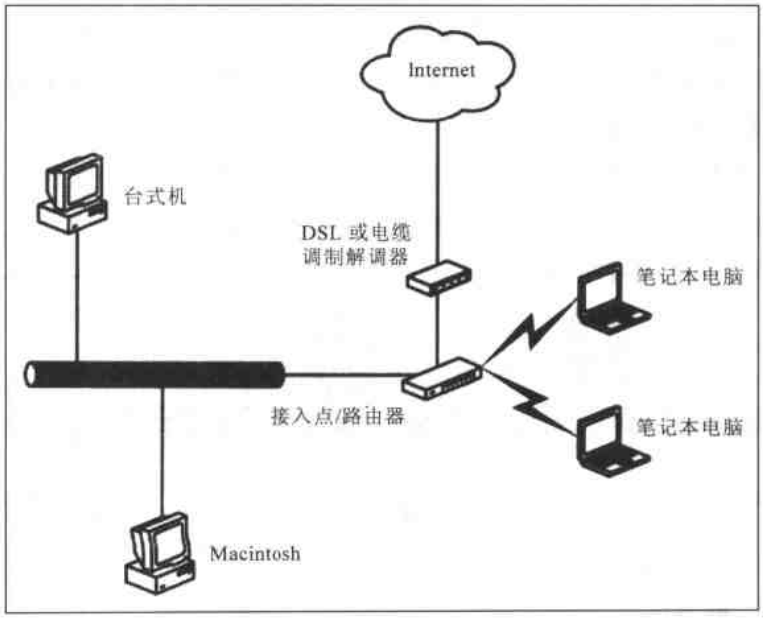

图 2-9　整合了宽带网关的无线接入点，可以支持共享高速 Internet 连接的无线网络

这个方法在家庭网络或小公司最为实用，其中宽带 Internet 服务的连接通向办公室，而不是止于服务入口或电话亭，因为接入点需要被放置提供无线网络覆盖的最佳区域。

2.5.5　多个接入点

单独一个无线接入点就可以在一个开放式相对较小且有较适中的网络通信量的空间里支持无线 LAN。但如果您的接入点需要覆盖较大的区域时(直径超过 100 英尺)，或是在一个满是墙壁、家具或其他物体阻碍、甚至有其他无线电干扰的环境里，您或许不得不增加一些接入点。

大多数家庭网络或小公司里的网络都只需要一个接入点就足够，因此选用一个支持漫游的接入点仅仅是为了解决很大并且复杂的网络才被考虑到。

802.11b 规范包含了一个漫游功能，当来自新的接入点的信号质量比原先要好时，会自动断开与原先接入点的连接而连接到新接入点上。当一个网络客户机连接到接入

点上时，它会自动地测试所有的无线电频道，以便确定是否有工作在其他频道的接入点能比现用的提供更强或更清晰的信号。当客户机找到一个能提供比现有更快的链接时，它会断开原有的连接，而立即连接到更好的信号源上。

因此，覆盖区域重叠的那些接入点应该被设定在不同的频道号上。为了将各个接入点之间的干扰降低到最少，每对相邻的接入点频道号应该隔开 5 个频道。

多数情况下，网络客户机不会连接到一个不同的接入点上，除非这个客户机移向一个不同的地方，而网络连接是活动的或者当前频道内信号流通量剧增。换句话说，当用户把笔记本电脑或 PDA 从一个地方移到别处或者当网络必须重新平衡各个接入点之间的负载时，就可能进行重新连接。

如图 2-10 所示，所有接入点必须通过一个传统的有线 LAN 连接在一起，在这个 LAN 里可能还有一些不需要无线连接的计算机或服务器存在。

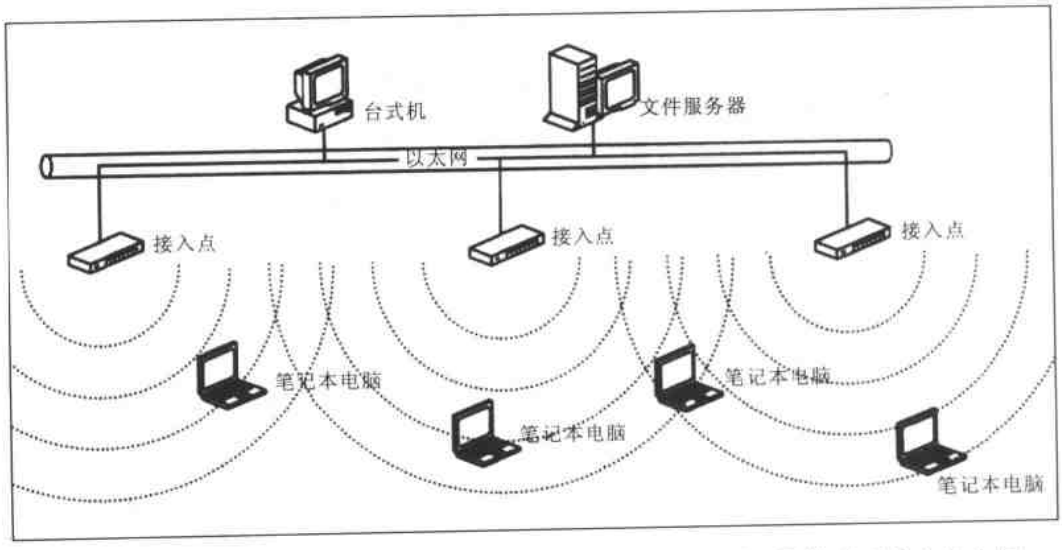

图 2-10　无线 LAN 中的多个接入点支持无线用户在较大的区域里漫游(优于单个接入点)

通常，多个接入点应该被放置在能覆盖其他接入点覆盖量 30%的区域。然而，如果您的无线网络必须支持多个并发用户，平衡负载的最好方法就是在同一地区安装两个或多个接入点，并且每个接入点被设定在不会互相干扰的无线电频道上。

802.11b 标准覆盖了漫游功能，因此可以在同一网络里使用不同品牌的接入点。它们被假定能相互协作运行。然而，每个接入点都有它独特的配置实用程序，或许还有不同的设计，因此使用一个品牌的接入点的网络通常要比混合的网络较容易配置和使用。构建一个无线网络是相当复杂的；能解决一个造成混乱的潜在问题源就已经很好了。

2.6　外置天线

如果用内置到网络适配器的天线和附加到接入点的固定天线(captive antenna)建立了一个到网络覆盖区域中所有地方的可靠的高速链接，那就没有理由再花时间、金钱和精力在外置天线上了。一旦达到可能的最大速率，再好的天线也无法提高数据的传输速率。

但如果接收条件不是很完美，而且您想把无线电信号发射到尽量远的地区，一根独立的天线就能切断干扰、增加数据传输速率、扩展网络覆盖区域和在有些普通内置天线根本无法传输到的地区建立可靠的通信链接。

乍看起来，提高无线电信号质量的最简易方法就是提高发射器的功率。大多数无线适配器的功率仅是毫无用处的 30 毫瓦(0.03 瓦)，为什么不再提高 10 或 20 瓦呢？这样是不是就能提供更强的信号呢？

显然这一方法可行，但 FCC 和其他一些管制无线电服务的机构规定了您不能这样做。更强大的无线电会产生更强的信号，但会对更广的区域造成更大的干扰，这也意味着更少的人可以共享同一段无线电频谱。相比之下，纽约电视台所用的频道 4 用 100,000 瓦的输出功率发射，而使用同样频率的最近的电台则在波士顿，两地距离几百英里远。无线 LAN 的无线电使用功率小于 1 瓦，因此信号根本不可能达到几百英尺以外。

既然不能通过提高无线电发射器的功率来增强信号，剩下来的也只有优化天线的性能了。

无线电天线有两种样式：从各个方向等强度发射和接收的全向天线和把能量和灵敏度集中在某个特殊方向的定向天线。在无线 LAN 里，使用全向天线的无线接入点在您想覆盖较宽区域时很有效。带有全向天线的网络适配器可以同等地和附近的接入点通信。如果您想把无线 LAN 覆盖的区域扩展到内置全向天线所不能达到的区域时，使用外置天线能增加 15%的覆盖区域。

换句话说，如果您的链接的信号质量在网络节点距离最近接入点 100 英尺左右就有所衰减，您可以在接入点或适配器中使用外置的全向天线，能使有用的信号区域扩展到 115 英尺。如果您在两端都使用外置天线，理想的距离应该是 132 英尺。当然，100 英尺仅仅是一个容易计算的例子。一对内置天线的实际信号区域很不相同，这取决于两个设备之间的阻碍和其他无线电信号的干扰，但使用外置天线肯定能够增加 15%的覆盖率。

定向天线的覆盖区域的形状和增益量(从发射器发出的信号强度和接收器的灵敏度)取决于每个天线的设计。有些定向天线能以较宽的模式(如泛光灯一样)提供适中的信号增益量，而有的则在某个较窄区域中集中了三或四倍(或更多)的增益。

定向天线可在紧密集中的覆盖区域中很大程度地提高信号质量，而且可以减少来自覆盖区域以外的“空”区域的干扰。这也决定了它们在无线 LAN 中的一些用途：

- 它们可以允许“正常”覆盖区域以外的用户连接到网络。
- 可通过在某个方向上减少覆盖而增加接入点所服务的有效覆盖区域。
- 可减少或消除来自其他无线电信号的偏离轴向的干扰。
- 可减少无线 LAN 对其他无线电的干扰。
- 可在建筑物间建立长距离、稳定、点对点的链接。

2.6.1 天线特性

外置天线的形状和大小可以多种多样。在您选择天线的时候，请先考虑下面几点：覆盖模式、增益、外形因素和抗天气干扰性。

1. 覆盖模式

每个天线的规格说明书上都有一个能显示天线覆盖模式的形状图。通常，覆盖模式可以分为全向型(在各个方向上均衡地收发信号)、定向型(在某个方向上收发最强的信号)和 8 字型(在天线前方和后方信号覆盖强而在两侧较弱)三种。

定向天线的目录单和规格说明书上应该还包括用度表示的孔径角度、波束宽度、或捕获区域。孔径角度是指包含天线最大功率覆盖区域或灵敏度的一段圆弧。例如一根天线的孔径角度为 45°，这就说明天线最大能覆盖到在它前方 45° 范围的区域。

方向型天线向所有方向进行发射，因此大多数厂家都会告诉您在多个平面上的波束宽度。如果当您想把接入点的天线放在墙壁、屋顶或塔上，而又想与地面上的网络节点进行数据交换时，这就非常重要。

2. 增益

天线的增益(gain)是指发射功率或接收灵敏度与标准偶极天线相比的比率(偶极天线是一根竖直、中心驱动和半波长的天线，比如用于 FM 无线电和调谐器的 T 形状的双向天线)。增益通常用 dBi 来表示(等定向分贝)。高 dBi 的天线比 dBi 低的天线的增益要高。

在天线的波束宽度和增益之间常有一个平衡。这主要是因为孔径角度较小的天线集中了相同功率(或灵敏度)到相对较小的区域。

3. 外形因素

2.4GHz 无线电的偶极天线大约有 1 英尺长，但用于获得增益和定向特性的反射器和其他元素则要长一些。多数天线在一个并不影响它们性能的保护表面中提供，这个保护表面可以使天线清洁干燥，而且您可以轻易地把天线装到杆子或墙壁上。

全向天线通常都是垂直的鞭状或杆状，直径大概两到三英寸。一些高增益的天线或许有两到三英尺长。户内使用的话(特别是采用下垂式天花板的屋子)，特殊的挂在天花板上的全向天线是用来构建无线网络的最佳选择。

定向天线可以有很多外形，包括抛物状的碟形天线和面板，在天线的活动部位后面都有一个反射器；类似于小型屋顶 TV 天线的天线；有几个发射元素的片状或面板状天线，通常在一个类似于烟雾探测器的扁平外壳上，或安装在可以更精确地调整天线的旋转轴上。

4. 抗天气干扰性

户外的天线通常都会需要某些能抵抗雨雪和能破坏构成天线材料的紫外线辐射的保护。因此，大多数厂家生产的天线都会为元件封上防护性外壳。

防护性外壳并不服务于户内天线，户内天线要尽可能不显眼。有些天线宣称能“户内、户外同时使用”，但如果把它们安装在室内的话只会徒增开销。

2.6.2　怎样选择天线

要记住没有必要安装超过您能真正使用的增益的天线。如果您已经通过一个低增益天线构建了一个清晰的连接，您的网络其实已经工作的很好了，数据传输速度也不可能再提高，这是因为只有接入点在负责发射和接收来自天线的信号。实际上，信号质量并不会因为天线的质量变化多少，因为好的天线必然会接收较多来自其他网络和 2.4GHz 设备的噪声和干扰。

如果没有什么特殊需求，那么标准的全向天线应该是首选。如果您确实需要一根定向天线，那么选择一个可以尽可能有效地达到你所期望的覆盖区域的天线。如果您不需要覆盖很宽的区域，不要去花很多钱购买高增益天线；能覆盖您的网络所有节点的增益天线可以很好地工作，甚至工作得比更高增益和更昂贵的天线好，因为增益再高的话，就会把信号发射到没有未经授权的用户那儿。

最好从您购买无线电设备的同一个厂家购买天线，这样可以避免一些可能发生的不同厂家产品之间不兼容等问题。然而，如果您的网络需要一些不能从您的无线电设备厂家得到的特殊天线时，那就需要向其他专门的经销商购买。

2.6.3　根据个人喜好来选择天线

有些无线网络设计人员和实验员已经设计了一整套自制的 2.4GHz 天线，仅使用了一些诸如空的 Pringles 马铃薯片筒这样的既便宜又容易获得的材料。我们将在第 10 章详细谈到它。

除非您已经有了满是工具和测试设备的实验室，而且您还特别喜欢那些马铃薯片做成的快餐，这些家制天线并不会比有着良好性能设计的商业天线有更特别的优点。如果您计算一下材料成本和花在安装和测试一根自制天线上的时间(包括您去往您所在地的硬件商店的时间，另外您还要在选择合适的安装支架上花掉至少 45 分钟时间)，去商店买一根天线花的钱就很值了。例如，可以花大约$50 从 HyperGain(http://www.hyperlinktech.com/web/antennas)那儿购得一个有着比标准自制产品更高增益的定向天线。

2.6.4 定向天线的用处

有三种使用定向天线的方法：用于接入点，用于网络适配器，或用于两者。

1. 用于接入点

用于接入点的定向天线可以在接入点覆盖范围中给所有网络节点提供更强的信号。因此，它可以到达远离接入点的用户，也可以提高较近用户的信号质量，其代价就是损失了一些不在天线覆盖区域里的用户。

在一个需要多个接入点才能较好地覆盖的网络里，在某个特定覆盖区域中使用定向天线的接入点会比全向天线效率高。如图 2-11 所示，定向天线可以把信号集中到需要使用的地区而不是把信号等方向的发散。在这个示例中，定向天线的覆盖角度是 90°，因此它可以触及到建筑物的内部，但它不会在用户不需要信号的地方消耗功率来发射信号。

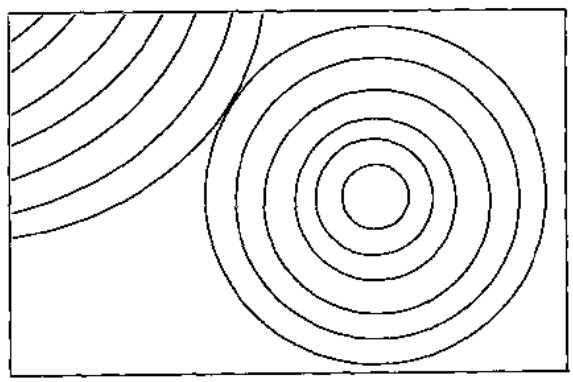

图 2-11　组合使用定向和全向天线可能是覆盖较大或特定区域的最好方法

定向天线还可以在一个方向上扩展覆盖区域，并且把信号发射到死点或是其他带有全向天线的接入点不能提供合适信号的地区。

2. 用于网络适配器

第二个选择就是把高增益定向天线放在无线网络适配器里，然后把天线朝向使用全向天线的接入点。这可能是通过还为其他更近的网络客户端提供服务的接入点将节点连接到网络上的最好方法了。为了避免安装其他接入点的费用和不方便，或是为一个用户单独走一根以太网电缆，可以尝试在这个用户网络适配器里安装一个定向天线。

3. 同时用于接入点和适配器里

在网络链接两端都使用定向高增益天线可以覆盖较广的区域。如果没有阻挡视线的树或者建筑物的话，一个从屋顶到山顶的链接可以达到几英里或更多。对于长距离链接来说，将两端的天线对准获得最大的信号强度非常关键：把天线稍改变一点角度可能会使原来很强的信号变得一点信号也没有。碟状或抛物状的天线的覆盖角度非常紧凑。

如果您把无线电链接的两个终端移开，会出现两个很复杂的问题。如果天线不足够高，地球曲率和 Fresnel Zone 电磁现象会干扰信号。在 2.4GHz，对于 1 英里的链接，两根天线的平均高度必须高出地面或其他阻碍物至少 13 英尺。要是五英里的话，最低高度就必须要 35 英尺，要是 10 英里的话，高度就要达到 57 英尺以上。

2.7　天线世界

在解决诸如提供接入到其他网络服务不可用的区域或把住得较远的用户添加进校园或合作网络里等这些特殊问题时，通常就需要长距离链接。在户内网络中添加覆盖一个死点的定向天线，或是装在屋顶或户外墙壁上为了覆盖一个停车场的面板天线，这些都不会使您的网络比使用配有全向天线的接入点来得更复杂。但是如果您开始想要那种复杂模式和高增益的天线时，一本只是讲关于无线 LAN 的书可能无法满足您的需求，您得寻求专家的帮助。

在安装一个大且功率高的天线前，您(或是其他为您工作的人)必须注意下面几个问题：防风性(您不会想您的天线因为一场暴风雨而倒掉吧)、本地政策(大多数人都把天线看的很丑或很危险)等。因此，他们有一些您在何处和如何安装天线的规定。而且您可能想要花一个较昂贵的测试设备(频谱分析器)来帮助对准两个天线。

如果没有这些经验，您可以寻求做这行或是做了很长时间测试的人的帮助。如果是您的一时冲动，希望您能一切顺利。可以在第 10 章找到更多关于长距离点对点链接的内容。

2.8 小结

这一章主要讲了一些不同种类的无线网络适配器、无线接入点和天线，利用这些设备您可以构建一个新的无线 LAN 或往您现有的有线网络中添加一个无线接入。下一步就是做一些选择然后购买这些设备了。现在可以安装这些无线硬件了。

在下一章里，您可以一步步地学到如何安装不同类型的适配器和接入点，然后运行配置实用程序，以便使这些硬件在网络中运行起来。

第3章　安装和配置接入点

在决定使用无线网络时，您至少有两个选择：打开所有的盒子，然后将无线电设备连接到计算机，试着将网络运行起来，或者是先进行一些计划工作，在开始使用这些硬件前先想好每个组件的最佳安装位置。本章是为那些先有计划再安装的人准备的，这些人都有很强的责任心，并且做事很有条理。本章也是为那些没有任何计划就尝试安装网络，而现在又想学习如何正确做好这项工作的人而准备的。

在无线网络中，接入点是与个人计算机和其他网络客户机交换数据的中央发射器和接收器。每个 802.11b 基础模式网络都必须至少包括一个接入点。其他的接入点可以增加网络服务的覆盖区域和支持更多的网络客户机，因此您的网络接入点的多少和位置直接决定了网络的覆盖区域和容量。

当您开始计划您的无线局域网时或任何局域网时，首先要做的就是多花点时间考虑一下准备如何使用您的网络。网络上的所有计算机是否都在固定的位置？是否都能方便地连接电缆？考虑使用无线网络是由于它是将计算机和用户加入到网络中的最佳方式，还是仅仅因为它是短暂的流行？

例如，我住在一个有未完工地下室的一层楼房屋中。我可以使用无线方式将家庭网络从前屋扩展到厨房(在我为这本书做测试时就这样做了)，但还有更简单便宜的方法，买一些便宜的以太网接口卡，然后从地下室的椽上拖一根 Cat 5 的电缆。另一方面，如果我需要在前门走廊或后院以及厨房使用笔记本电脑，或者我住在一个无法进入地下室或阁楼的两层楼或公寓房间中，我就可以在前屋安装一个接入点，并在笔记本电脑上装一个无线网卡，这样我就可以将我的笔记本电脑带到各处使用。

您可以对一个商业网络进行同样的分析。只要在办公室或工厂里的计算机都是固定的，并且您可以很方便地布置电缆，有线网络就是较好的选择。但如果销售人员在会见他们的客户时都带着移动设备，或者是工程师想在会议或午饭时间使用笔记本电脑时，又或者有其他原因要将网络扩展到有线网络无法达到的区域时，您就应该添加无线接入。

3.1　接入点的使用量

一个简单的无线网络仅仅操作一个网络接入点和一堆网络节点。然而，如果您想覆盖范围很大的区域、或是有会阻碍信号的墙壁或其他物体的区域时，您将不得不至少

添加一个接入点。

在一个复杂网络中，每个接入点所在的最好位置和放置单个接入点的最佳位置相近。如果网络覆盖较广，您可以按照相等间隔来放置它们，但是要找到覆盖一个不规则区域的最佳方法就太困难了。

放置接入点严格来讲并不是门科学。可能最好的方法就是从一个建筑物的一头放置一个接入点开始，然后确认它是否能适当地覆盖 50-100 英尺的区域，或是直到墙的第一转弯处，然后围绕运行站点测量程序的计算机放置。如果信号发生衰减，就立刻回到原来信号较好的位置，然后在相反方向的同样距离上放置另外一个接入点。如果第二个接入点没能达到剩余空间所必需的覆盖率，您可能不得不加入更多的接入点。您的目标就是在任何两个接入点之间最大只能有 30%的覆盖重叠。

放置三个或更多的接入点可能会变得凌乱，因为它们不再像一个或两个单元那么简单。记住，您添加多个接入点的目标就是尽可能地覆盖更多空间。在一个开放空间中，如果有两个接入点，您可以在两边的墙壁中间放置这两个接入点，距离大约为前面和后面墙壁之间的三分之一远。如果要添加第三个接入点，您可以将这个接入点放在两个墙壁的中间，并将先前的两个往两侧墙壁靠近，或是将它们组成一个三角形也可以。

如果在一个复杂空间中需要两个以上的接入点时，您可以考虑组合使用全向天线和定向天线，而不是仅仅在某些接入点中嵌入全向天线。覆盖一个死点或是将网络扩展到一个建筑物角上的最好方法就是将天线架在高墙上，并且让它向里面传播。请特别注意天线的覆盖模式，因为它可以是一个很紧凑的圆锥形，而不是一个宽弧(想想泛光灯和聚光灯就可以知道两者的差别)。

那么可不可以避免在天花板上盲无目的地爬上爬下，将接入点不停地换地方进行测试呢？我能提供的最好建议就是做好平面计划。裁出一些相等半径(100 或 150 英尺)的圆，其他地方则尽量符合定向天线的覆盖模式，接着围绕平面图上不停地移动它们，直到这些位置的组合能达到最大的覆盖区域。这个方法可能比较粗糙，但应该可以作为实际站点测量的好的开端。

使用网络的人数也会影响所需的接入点数目。这儿有一个实际的限定：如果有超过 6 个计算机尝试同时连接到一个接入点上，每个无线节点的数据传输速率就会开始下降，但记住大多数用户并不会总试图在一个给定时间中传输数据。同一时间内的“6 个”用户可以理解为一天内的 20 或 30 个用户。

如果网络的用户数量不断增加，您可能就会发现网络性能开始下降，这主要是由于接入点几乎是在满负载工作。如果真的发生了这样的情况，您就必须考虑在您的网络中添加新的接入点。您可以在现有的接入点中间放置新的接入点，也可以直接放置在现有接入点的附近。如果有可能，将新的接入点设置到没有干扰的不同频道数上，然后将半数的网络节点都设置到这个频道上。

如果以基础模式工作，您的网络类似于一个星形拓扑设计，其中每个节点都通过接

入点与网络进行通信。因此，没必要将您网络上的所有节点都设置使用一个频道。如果能将节点分布到两或三个不互相干扰的频道上，就可以减少每个频道上的链接数量，这样也会改善网络的整体性能。

3.2　执行站点测量

一般性的原理总是很完美的，但您是在由真实的墙壁和家具构成的位置中安装您的无线网络(而且可能会有干扰源)。无线电波会穿过某些物体，而在有些物体上反射，因此在一个理想环境下，对无线电射程和信号强度的一般性预测没有在您想要使用无线电波的环境下的实际性能来得重要。您所需要的就是一个站点测量，该将告诉您无线电在您自己空间中的工作方式。

执行站点测量的第一步就得确定您的网络想要覆盖的区域。大多数情况下，这个区域会是您的办公室、家庭、校园的所有区域，但还有其他可能。例如，您或许只想在一些公共区域(诸如会议室、招待所或图书馆)中提供网络连接，或者您想与一群邻居共享一个宽带网络连接。记住，2.4GHz 的无线电信号可以穿过大多数墙壁、天花板和地板，因此它们可以到达附近的空间，即使您并不想将它们发射到这些区域。

对于一个家庭或小型办公网络，您的站点测量可能很简单。如果整个建筑物仅仅为 50 英尺长和 30 英尺宽，那么您可以将接入点放在任何地方。只要将您的接入点连接到现有的 Internet 连接上，您就可以将笔记本电脑或其他移动计算机作为网络客户机，并且当网络连接被激活时可以将这些设备随意移动。如果您能在家里或办公室里保持网络连接一直通畅，那么一切就绪。

一个网络覆盖的区域可以是不连续的(或是邻近的)，尽管大多数网络构建采用连续方式。例如，您的办公地点可能在大楼的三、四和九层，但四到九层中的任何一层都不是。在这个情况中，您可以将接入点放在自己的办公室里，使用以太网电缆将它们连接起来，这样就可以忽略其他层了。如果您的局域网要扩展至多个建筑物，若没有现成的链接您可以在每个建筑物里放置接入点，然后用租用线路(Internet 上的虚拟专用网络(VPN)，或是通过点对点的无线电链路)将它们链接起来。

3.2.1　计划站点

如果您已经对网络需要覆盖的区域有了一个大体想法，那么就应该创建一个更详尽的平面图。如果网络要覆盖建筑物的几个楼层，或是您的网络将包括好几个建筑物，您就应该对每个楼层制定一个计划，并且为每个建筑物做一个纵向图，另外再做一个能显示网络整个覆盖区域的图。

您的楼层平面图应该包括每个墙壁和隔板、现有网络连接和交流电源插座等位置。如果您知道一些潜在的干扰源，比如 2.4GHz 无绳电话、蓝牙网络或微波炉，也将它们的位置标在图上。图 3-1 给出了一个小型办公室的楼层平面图。

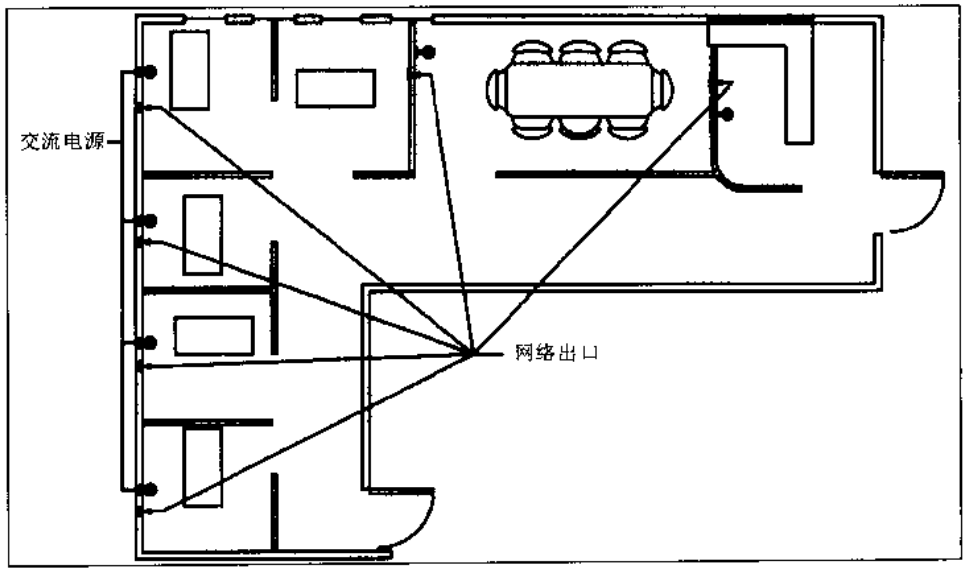

图 3-1　一个办公室楼层平面图

通常，如果您用眼睛能看到所有想放置计算机或网络客户机的位置，您就可以只用一个网络接入点。如果因为有一些无线电信号的阻碍物而不能直接看到一个位置，您可能需要增加接入点，但不要盲目地认为一条无阻碍的无线电路径和一眼就能望到的路线一样。惟一的方法就是启用一个接入点，然后运行您的测试程序。

在图 3-1 所示的办公室里，能一眼看到所有方位的最佳位置可能是 L 型空间的角落。如果那个位置还不合适，另外一个方法就是将接入点放在办公室的两头。这个办公室里有很多网络转换器和交流电插座，因此连接一个有线网络应该不是问题。但这并不代表这个方法永远都是正确的。在很多地方中，放置接入点的合理位置应该是在人工的天花板中，但如果您不能将交流电插座接到那儿，您将不得不另外找个地方，或者用一个支持通过以太网供电(PoE，Power over Ethernet)的接入点。

如果较好的接入点位置靠近交流电插座，但离网络连接点较远，这一般不会有什么问题。您可以使用一根很长的数据电缆来解决这个问题，但千万不要直接从人工的天花板上将线拖到房屋中间或是不能到达天花板的隔板上；这看上去很乱，有人最后总会猛拉它。如果您将数据电缆延伸到实际墙中，然后从墙中走线，或是将它放到两个墙壁相接的角落上，这样就显得好一点。记住，传输高速数据时最好不要在尖锐的角落处转弯；所以务必在电线从水平方向改到垂直方向时放一段较宽的曲线。

如果您想用一个接入点来为一建筑物两个邻接的楼层服务，最佳的位置就是靠近公

用天花板和地板的地方。在很多房间中，这一位置并不是关键性的，因为无线电信号可以很容易穿透木质材料和石膏，而穿过水泥和钢质材料就比较困难。

如果要使您的室内网络的预期覆盖面积扩展到离接入点的距离大于 150 英尺，就该考虑使网络用多个接入点。而在户外，您就可以从最少 200 英尺以外的接入点获取很可靠的信号，当然这个前提是您能一眼看见那个地方。

大部分接入点和网络接口的内置天线都是全向的，这也就意味着它们向各个方向同等地发射。换句话说，有用的信号所覆盖的区域就像一个球面或油炸圈饼，而天线被放置在中央。因此，您期望将接入点大概地置于您将覆盖的区域的中央。如果您使用的是一个还有外置天线连接器的接入点，您就可以更灵活地按照上述方法操作。在一些环境中，被放置在建筑物一端的定向天线应该比放置在中央的全向天线效率更高。

许多接入点上的内置天线是安装在旋转轴上的鞭状物，您可以相对于装有该回路的盒子来改变它们的位置。这或许没有什么不同，但是，当接入点被放在靠近天花板或接近地板上的位置时，您就可以将天线直接朝向下方。而通常来说，将天线垂直放置会比水平放置增加天线的覆盖率。

另一个可能导致信号丢失的潜在原因是多径干扰。多径的丢失发生在直接从发射器传来的相同信号到达接收天线时，还有一个反射表面反射回来的第二波信号。在一个广播电视信号中，多径在屏幕上以重影形式出现。在一个包数据网络中，接收器会将多径干扰当作噪声处理，这同时也减慢了数据传输的速率。

多数网络接入点和无线适配器都在分集接收排列中使用两根分开的天线，从而降低或去除多径干扰的影响。接收器比较两根天线的信号强度，自动选择信号较强的一根天线。即使这两根天线距离一到两英寸，分集系统仍然会比单个天线提供更为清晰的输出。如果接入点的内置天线被放在一个形如不规则 U 形条的包中，或者在一些 D-Link 接入点中，它们都有两根分开的天线，这样的装置大概就是使用了分集接收系统。检测硬件是否使用分集系统的最好方法就是看它的说明书。

如果您的网络接入点有两根固定天线，您或许想对不同的天线相对位置作个测试，如果天线平行于南北放置时，您的覆盖率就不会高，试着在您观测一个网络客户计算机上信号强度的同时逐渐改变接入点的方位。如果天线被放置在旋转轴上，不要将他们绝对平行放置，而是试着将他们来回转动一下。

户外的基本规则就是“越高越好”。尽可能使用带有外置天线连接器的接入点，这样您就可以将盒子放置在屋内，然后将一根同轴电缆拖到天线处就可以了。一个能放置在屋顶上并且抗天气干扰性的垂直天线，或是能高架在建筑物一侧的平板天线，都能提供大概 300 英尺的覆盖区域。当您将天线放在屋顶上时，尽量将它架得高一些，以便您能从地面上直接看见它，这样就可以减少建筑物本身造成的信号衰减，如图 3-2

所示。如果您不能看到接入点的天线，信号质量就会受到影响，但还是要通过这样的结构才能接收到足够的信号。如果您在 20 英尺以外收到的信号比在墙角边收到的信号还强，这一点都不奇怪。

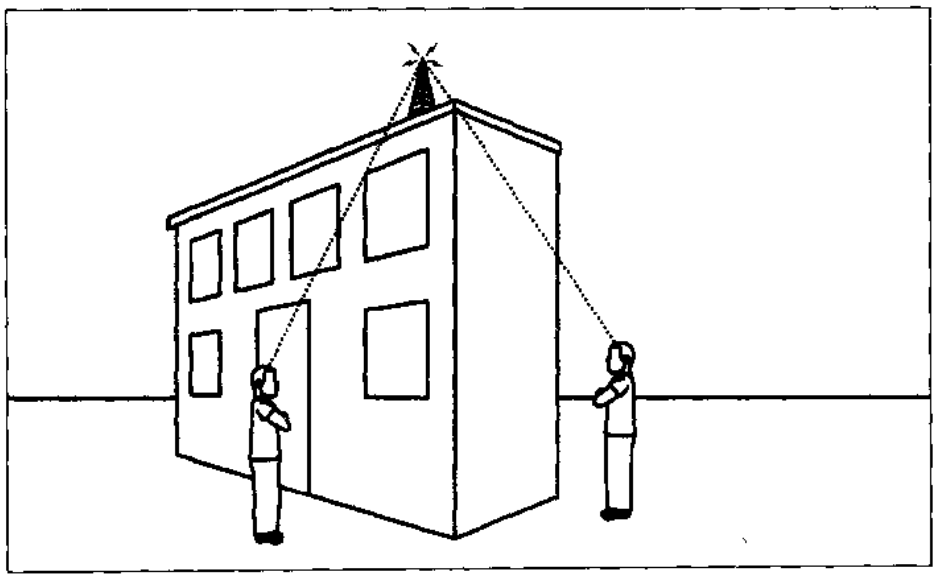

图 3-2　一个屋顶天线可能不能覆盖到靠近建筑物的人

受结构影响所造成的信号衰减量因不同的建筑物材料而不同。2.4GHz 的无线电波能轻易地通过木材和玻璃，而通过水泥和钢质材料时就比较困难。从实际的角度出发，如果并不是试图使用您的无线网络覆盖一个很大的大学校园或工厂，您就可以从户内接入点获得完全有用的户外信号，特别是接入点被放置在靠近外墙的地方。如果您正在做站点测量，那么可以在网络连接被激活时携带一个可移动设备远离建筑物；您可以很惊奇地发现信号竟然能发射这么远。

请记住，我们正在讨论数字信号。一旦我们已经获得能提供清晰且高速的数据链接的最低信号质量，除非您遇到干扰问题，那么就没有必要使用更强的信号。如果您已经能从已有的户内接入点覆盖到户外野餐用的板凳上，那么就不需要在添置户外接入点上浪费金钱和时间。户外的接入点可以得到更强的信号，但是它并不能提高数据的传输速率。

如果将机车或是其他大型金属物体(如建筑用的起重机)移到接入点和网络客户端的中间，这就会阻碍清晰信号的路径，并且产生暂时的信号丢失。如果您想将信号覆盖到货运场或是卡车等大型物体来回走动的其他地方，可以将天线尽可能地架高，然后在您想覆盖的区域的另一侧再放置一个接入点。

3.2.2　测试，再测试

完成所有理论性计划后，您必须使用实际的硬件来进行实际的测试。一个楼层平面图或许可以让您理解网络如何工作，但要弄清楚网络覆盖区域的无线电波传输方式就必须安装一些暂时的部件，然后进行一些实际测试。

在必须执行站点测量时，您可以有三个选择：

- 让别人为您做这件事——可以是需要付费的顾问，或者是想要卖给您网络设备的供应商。
- 利用一些无线硬件所提供的站点测量软件。
- 利用网络接口提供的配置程序或状态程序。

请一个顾问或销售方的技术员为您测量可以有很多好处。首先，您可以让这个人做这项工作，而您只要记下报告就可以，而不必在大楼里带着测试设备跑来跑去(或者是爬)。更重要的是，做站点测量的人员都有他们自己的设备，可以自动存储一些个别的读数和提供详细的报告。遗憾的是，这些设备非常昂贵，而且也要有特殊的培训，因此对一个临时用户来说就很不实际了。

如果找不到其他人来做这项工作，您将不得不自己去做。很多硬件制造商，如 Cisco、Xircom、Proxim 等都随它们的接入点和网络适配器一起提供了站点测量软件工具。图 3-3 显示了一个正在运行的 Xircom 站点测量程序。

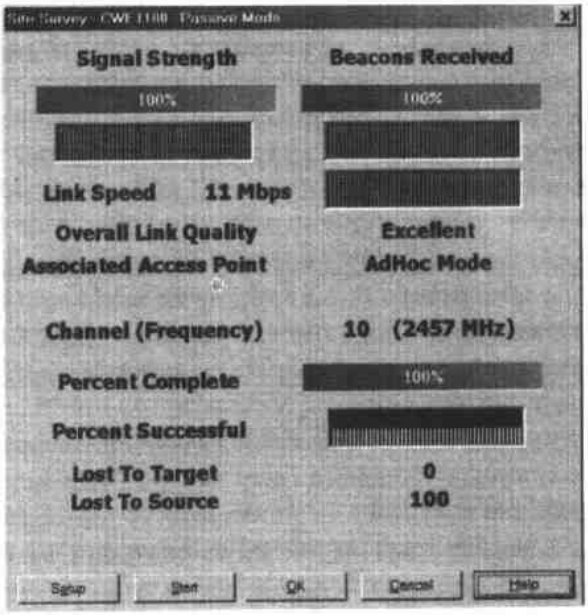

图 3-3　显示您想测试的网络信息的站点测量程序

如果测试硬件没有这些工具，您可以从每个无线接口自带的标准状态和配置程序中

获取足够的信息来做站点测量。使用测量工具可能要简单些，但配置程序也可以告诉您需要知道的内容。

最有可能的是，您测试的第一个接入点就有一个完全覆盖度，特别是在网络很小的情况下。但如果您要建立一个较复杂的网络，有时候就要说服网络提供商允许您测试一下来自不同厂家的网络接口和接入点。因为不同厂家使用不同的天线设计和配置软件，您或许会发现某种型号的网络适配器和接入点工作得较好。

下面是做完整的站点测量所要做的事情：

(1) 选择接入点的位置。您或许决定做好站点测量后再改变它的位置，但当开始时，最好选择一个能一眼看到尽量大网络覆盖区域的位置。

(2) 如果已经有了合适的有线 LAN，将您的测试接入点连接到该局域网上，然后接上电源。如果没有一个现有的局域网，那么先连接上电源，然后开启接入点。

(3) 在笔记本电脑上安装一个无线网络适配器。如果接入点没有被连接到有线局域网，那么在另外一台计算机上安装另一个网络接口。第二个计算机必须靠近接入点，这样可以得到一个清晰的信号路径。

(4) 使用接入点和接口适配器的配置工具来确保它们工作在有着相同 SSID 号和前导长度的相同频道上。将接入点上的适配器软件和配置实用程序设置为基础模式，然后将传输速率改成 11Mb/s 或自动。进行这些测试时，要关闭 WEP 安全性。

(5) 根据楼层平面图，准备一个如图 3-4 所示的站点测量表格。在位置栏中将您覆盖区域里的每个房间作为一项；较大的空间可以用两到三项来表示。

位置	信号强度	信号质量	链接速度
会议室北端			
会议室南端			
接待区域			
Mike 的办公室			
Sarah 的办公室			

图 3-4　一个无线网络站点测量表格

(6) 将笔记本电脑放到测量表的第一个位置。

(7) 在笔记本电脑上运行站点测量程序、配置或状态显示程序。程序应该能报告出网络节点和接入点之间的信号联接，以及信号强度和质量。有些程序只报告强度或质量，但并不会同时报告这些信息。图 3-5 为一个配置实用程序显示，包括了 Link Quality(链接质量)和 Signal Strength(信号强度)的信息。

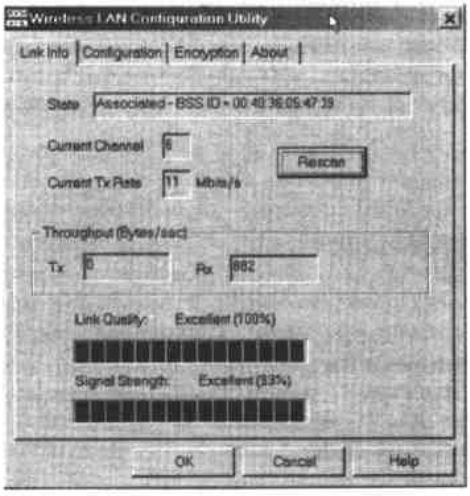

图 3-5　显示无线连接的信号强度和质量信息

(8) 有些配置程序仅当有文件传输时才测量信号质量。如果程序没有显示任何信号，请打开 Windows Network Neighborhood 窗口(如果您正在使用 Windows)。当计算机开始访问网络时，无线程序会显示信号强度和质量。如果您的移动设备仍不能与接入点连接，阅读硬件自带的手册，由此可获得更多关于设置网络硬件和配置计算机来连接到无线网络的信息。

(9) 将当前位置的信号强度、信号质量和链接速率复制到测量表格中。若未使用站点测量工具，您的显示信息可能不会包括链接速度。

(10) 当状态或配置程序运行时，将笔记本电脑移到表格中的下一位置。如果有必要，使用 Network 窗口中的 Refresh 命令来获得新信息。注意测量表格中的强度、质量和链接速率。

(11) 在表格列出的每个位置中重复上述过程。

您或许还想在建筑物间转转，在您走动时信号质量无变化。如果您渐渐远离接入点，您可能猜想信号强度会慢慢降低，但如果信号质量和 ping 速率的数值仍然很好(低的 ping 速率会好一些)，您就不应该对在这个地方使用无线连接产生怀疑。

如果您发现存在一些死点，这些区域的信号强度和质量已经降到一个不能使用的级别，这时请不要奇怪。因为在接入点和移动设备之间有障碍(例如一个金属档案橱柜)或附近有一些本地干扰源(例如一个微波炉、蓝牙设备或无绳电话)，这些死点就会产生。查找这些死点也是做站点测量的原因之一。在有些情况中，从您原先的位置移开一到两英尺就可以解决问题。在表格中一定要标注上这些死点的位置。当在建筑物内移动时，您发现了大量的死点或是这些死点在一些重要的位置，那么就有必要挪动接入点。

在您测试完表格中所有位置的信号质量之后，在楼层平面图上标注接入点的位置，并复制每个房间或其他位置的测试数据。如果您在一个相对较小的空间里工作，您会发现大多数位置都有相近的数值。不要对离开接入点很远地点的信号强度下降很多感

到奇怪。如果信号质量和速率降到不可使用的级别，您或许要增加一些接入点。

如果在您想要覆盖的大多数区域中的信号质量都不能达到可使用的级别，将接入点放到其他地方，或是如果接入点还有另外一根外置天线，移动一下天线。尽可能再找一个有着尽可能大的清晰和无阻碍的视野的位置。重复新位置接入点的测量工作。

3.2.3 总结：站点测量步骤

(1) 确定您想让网络覆盖的区域。
(2) 准备楼层平面图和垂直图。
(3) 选择接入点和天线的最佳位置。
(4) 与其他无线网络协作。
(5) 安装接入点。
(6) 从多个位置测试无线连接。
(7) 尝试移动接入点或天线。

3.3 干扰问题

如果半英里内没有其他人使用无线网络或其他 2.4GHz 设备，您就不需要担心您的网络中会有干扰。这个可能性每天都在减少。其他网络服务以及无绳电话、微波炉、户外照明系统和无线电控玩具，它们都使用同一组频率。一些附近的家庭或办公室网络或许也在尝试使用他们自己的 802.11b 网络。因此外面就像一个无线电丛林。

无线以太网络使用的无线调制类型可用于消除来自其他服务的干扰。但那只是理论上可行。设计不同 2.4GHz 无线电服务的工程师一直在尝试互相协作，这样我们可以同时使用网络、电话、微波炉和无线电控玩具。然而实际上，接入点和网络适配器中的接收器可以监听一个频道，该频道可能包含一个好而清晰的 Wi-Fi 信号，然后就如同将他们的手举向空中喊“Arrrgh”一样执行数字信号。

或许可以更精确地说，它会将一条消息发送回信号源，“嗨？您在说些什么？我不能明白最后一个包中的内容。”如果发生这样的事，发射这个信号的无线电会将相同的包重复发送，直到接收方确信它收到一个清晰副本。下一个包发送也同样遵循这个过程，然后一个接一个。这就像通过一个嘈杂的电话线或者说无线电话机打电话一样，其中...您...必...须...说得...很慢...而且...听得...很...仔细。换句话说，本来良好、高速的网络现在感觉起来就像正在从一个充满渣滓的管道里接收数据位一样。

如果在您周围有很多无线电干扰，您将可能在做站点测量时发现它们。如果在到接入点的清晰视线上不能建立起 11Mb/s 的连接，您可以寻找附近的其他信号源。这可能

是一些很显然的事物，如您的餐厅中的微波炉，或者厨房中的无绳电话，但其他东西就不容易被找到，如附近的无线网络，或是穿过您房顶的无线电链接。

您可以使用一些方法来减少或去除干扰：移开干扰源或将您的网络移到其他频道上。改变频道一般更容易，但它并不总是有效，因为您的干扰源可以是在整个 2.4GHz 频带上跳换的跳频无线电，或是工作在新频率上的完全不同的信号干扰源。

根据以下的步骤来消除干扰：

(1) 换到其他频道，至少与现在您遇到问题的频道相差 5 个频道。例如，如果不能使用 6 频道，那么可试着调低到 1 频道或调高到 11 频道。

(2) 寻找一些在 2.4GHz 发射的无绳电话、微波炉或其他设备。如果可能，使用那些在不同频率工作的(例如工作在 900Hz)的无绳电话来换掉这些干扰设备。

(3) 如果可以改变接入点和适配器的无线电输出功率，确保将它设定在较高的设置上(100mw)。

(4) 询问您的邻居是否正在使用无线网络。因为他们很可能也和您一样经历着您的网络带给他们的干扰，他们会在频道分配计划上和您合作，不同的网络使用不同的频道。记住，如果您们能保证至少 5 个数的频道间隔，那么就可以将频道交叉干扰降至最低。如果您要协调的频道多于三个，那么将这些频道位数分得越开越好。因为三个频道中惟一不会相互干扰的一组频道是 1、6 和 11，所以您会发现它们包含的来自邻域网的干扰比任一个中间频道都多。您可以在一个或两个中间频道找到合适的分配。

(5) 用可以增加信号强度和接收器灵敏度的定向天线替换接入点或(和)网络适配器的全向天线。您或许不得不将接入点移到其他地方，或增加一些接入点来覆盖相同的区域。如果您能说服您的邻居使用定向天线，尝试将这些天线进行排列来最小化重叠覆盖区域。

若上述方法不能奏效，除了接受更差的性能或将 2.4GHz Wi-Fi 网络换成运行在 5.2GHz 的 802.11a 无线网络之外，您别无选择。

您可能还会遇到更多的干扰源，但这些干扰源可能直到您运行网络一段时间后才会发觉。随着您的无线网络在用户中变得更为流行，越来越多的用户会在同一时间使用网络，这样整个网络的性能肯定会降低。为了解决这个问题，您可以增加一些工作在不同频率的接入点。

3.4　安装接入点

像第2章所讲的，多数接入点可以和其他无线设备组合，如网络路由器、宽带 Internet 路由器和传统的以太网集线器。在最低配置时，每个接入点都会包括一个无线电发射器和接收器，以及一到两个固定的天线或外置天线的连接器，将接入点连接到有线网

络的以太网端口。接入点还包括一种内置的配置软件，它显示了当前的设置，并且能接受改变设置的命令。

因为每个接入点都会随着不同的输入、输出和控制产生不同的数据包，您或许会希望按照设备所提供的特定安装和配置说明来安装。遗憾的是，生产厂家的手册并不总能提供您所需要的信息。这一节会告诉您安装常见接入点的一般步骤，同时还有一些不是每个设备都会有的特点和功能的提示。这些都可以用于补充您的接入点手册里没有讲到的安装过程。

3.4.1 物理安装

下面是安装接入点的一般步骤：

(1) 如果需要，组装接入点。接入点用户手册应当包括一些正在使用的型号和模型的特定说明。

(2) 根据站点测量所得到的信息将接入点放置在您所设计好的位置。

(3) 如果接入点有一个安装在旋转轴或是其他能让您改变方向的部件上的固定天线，尽可能调节天线到垂直位置。如果您将天线放在天花板上或是靠近它，那么就尽可能将天线垂直向下放置。如果天线靠近地板，那就将天线往上垂直放置。如果不能调整天线的方向，也不需要担心：接入点通常在固定的位置也能良好地运行。

如果接入点有一个外置天线的连接器，那就先安装天线，然后从天线拖一根到接入点的电缆。使接入点和天线之间的电缆尽可能短，这样可以避免拉扯或有什么尖锐的转角。

(4) 将接入点接上电源。多数接入点都提供壁式直流电适配器，但有些使用交流电线。不管是何种电源，首先将电源线接到接入点上，然后将电缆和电源插入交流电插座中。

接入点不会耗费很多电，因此没必要专门准备一个交流电源，但如果您使用不间断电源或浪涌电压保护器来保护您的计算机，您同样也要保护您的接入点。

如果您使用 PoE 系统来为接入点提供电源，按照 PoE 提示将您的接入点接上电源。

(5) 在接入点的局域网连接器和最近的网络集线器、交换机或其他网络节点之间连接一根以太网电缆。

(6) 查阅手册可以知道如何将控制电缆接到接入点。有些接入点使用来自于附近计算机的串行电缆，而其他接入点则通过网络进行连接。您将使用这种连接来设置接入点的配置。

如果接入点使用串行连接，您可以更容易地将您的笔记本电脑带到接入点附近的临时位置，在其中可以看到 LED 指示灯，在运行配置例程时变暗，而不是拉一根更长的电缆到已有的计算机。

(7) 打开接入点的电源开关。您或许会看到一个 LED 指示灯。接入点的内部处理

器准备运行要花点时间。接入点的帮助手册会说明那些指示灯的功能。

在您完成物理安装后，下一步就是配置接入点了。如果您使用相同品牌的接入点和无线接口适配器，这些设备的默认设置都应该一样，这样您可以在另外一台靠近的计算机上安装适配器，然后就可以马上测试网络。

3.4.2　通过浏览器来配置接入点

多数接入点都有有线局域网端口，因此它们通常都可以通过专门的本地数字 IP 地址来接受配置命令。可以用 Microsoft Internet Explorer，Netscape Navigator 或是其他图形 Web 浏览器来察看或改变接入点的设置。接入点里也包含一些自己的软件，因此它的配置程序可以运行在任何一个操作系统中。没必要为 Windows、Macintosh、Linux、Unix 或其他操作系统寻找不同的程序。

多数人将发现图形配置实用程序比命令行版本更易于使用，因为在您想做任何事时，您不需记住许多含义模糊的命令。

当您第一次打开接入点时，它会使用出厂时的默认设置。如果不改变其中一些设置，就可能会让未经授权的用户访问您的网络，或是让其他网络(授权的或未授权的)用户改变接入点的设置，而这本来只能由网管去做。

同样，特定的配置过程因接入点类型而异，但通常原理都是类似的。使用下面的过程来补充接入点手册中的相关信息：

(1) 确认接入点被连接到局域网上。

(2) 从一个连接到局域网的计算机中打开您的 Web 浏览器。

(3) 在浏览器的 Address 栏中输入接入点的默认数字 IP 地址(像接入点手册中指定的那样)，然后按 ENTER 键。

(4) 浏览器会寻找和打开接入点的登录窗口，如图 3-6 所示。输入需要的信息，通常是登录名和(或)密码。

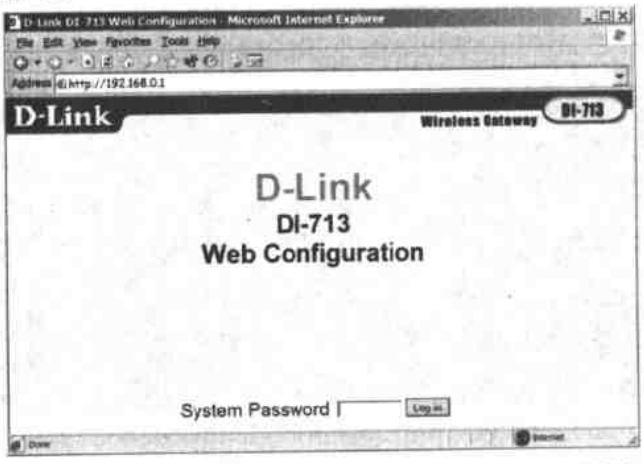

图 3-6　一个接入点的密码窗口，由此可以进入配置程序

(5) 您应该查看最上层的配置页面。图 3-7 显示的是一个典型的配置页面，它来自 ZoomAir AP11 的接入点。

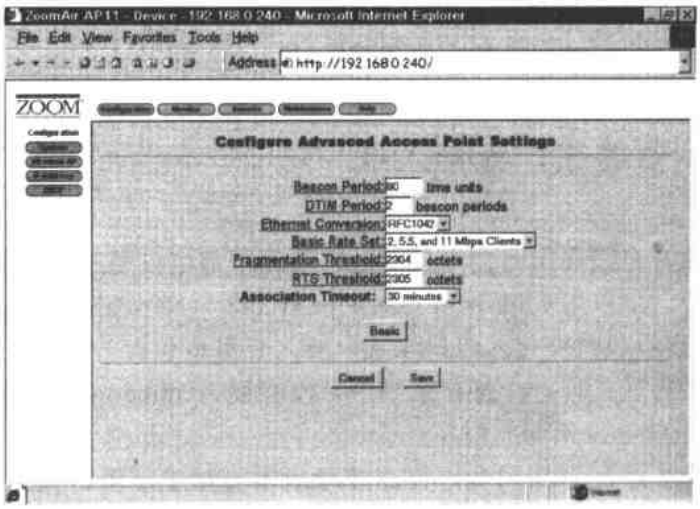

图 3-7　ZoomAir 接入点的配置屏幕，其他接入点的配置屏幕显示类似的信息，但排列的位置有所不同

如果您试图打开配置程序时接收到的是“Unable to connect”信息，而不是登录窗口，试着对接入点发送一个 ping 命令。在 Windows 中，您可以打开 DOS 提示窗口，然后输入：

ping [IP address]

这里的地址就直接键入接入点的数字 IP 地址。如果网络能识别这个地址，您会看到如图 3-8 所示的响应消息。如果程序报告“host unreachable”，这可能是局域网服务器上的动态主机配置协议(DHCP，Dynamic Host Configuration Protocol)和默认的接入点地址有冲突。下一节将解释如何处理这个问题。

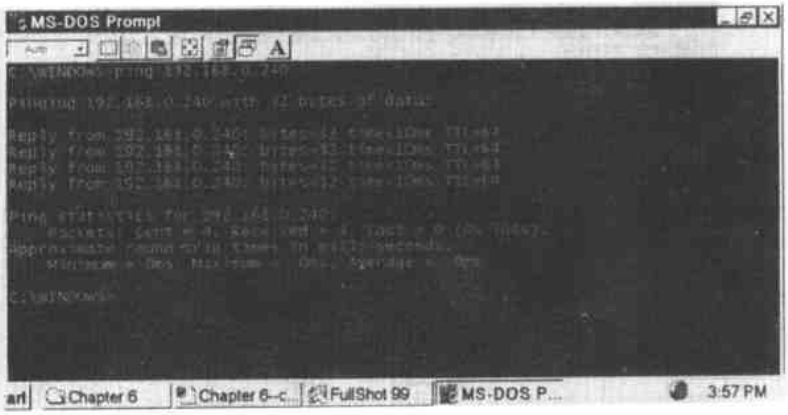

图 3-8　ping 请求成功后返回来自于目标设备的一系列时间响应

3.4.3　DHCP 和其他问题

DHCP 自动为网络上的每台计算机分配 IP 地址。因为无需为每台计算机手工分配单独地址，这样可以省掉很多时间和麻烦，但当网络的集线器或交换机和无线接入点都作为 DHCP 服务器，或一个客户机设备想要一个特定的地址，而 DHCP 服务器临时分配一个地址，安装网络就很困难了。

在您向局域网中加入一个接入点时，产生冲突的 DHCP 服务器会带来很多问题。一些单机的接入点希望使用一个特定的数字 IP 地址来访问基于 Web 的配置屏幕。如果接入点被连接到一个作为 DHCP 服务器的集线器上，这样服务器就会为接入点分配一个不同的 IP 地址。因此，当用户试图连接到接入点手册中所列出的 IP 地址时，除了显示“Unable to find this address”之外不会显示其他信息。

如果每个接入点使用同样的方式处理 DHCP，那么为接入点配置 DHCP 就会容易很多。但它们并不会这样做。这种情况只会发生在公司里所有设计和制造接入点的工程师都提出了相同的解决方案，但通常这种情况很少。

下面提供了一些解决这个问题的方法。您可以用多数接入点的控制功能来完全避免它，然后通过串行端口(而不是基于 Web 的实用程序)输入配置命令，但这意味着您必须使用比图形实用程序更晦涩的命令语言，并且很多接入点不能通过串行端口接受命令。

第二个可能性是使用控制功能来将基于 Web 的实用程序的数字 IP 地址默认值改为由 DHCP 服务器分配的地址。多数 DHCP 服务器能显示已分配地址的列表，如图 3-9 所示。在改变接入点地址之后，使用 Web 浏览器就可进入配置实用程序。

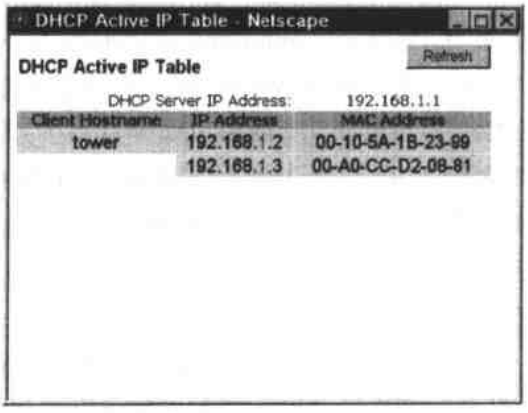

图 3-9　DHCP 服务器为局域网中所有节点分配数字 IP 地址。在这个示例里，接入点的地址是 192.168.1.3

如果您不想在设置接入点的串行端口连接时遇到麻烦，另外一个选择就是关闭 DHCP 服务器，然后使用接入点的默认 IP 地址在浏览器中显示您的配置实用程序。这

个方法只有当您正在安装网络时暂时可行，但它禁用了所有从相同的 DHCP 服务器接收分配地址的其他客户计算机的地址。因此，有必要手工分配地址或者确保在您完成网络配置后将 DHCP 服务器重新开启。

如果所有的方法对您来说都显得很复杂，还有另外一个进入配置屏幕的方法：从接入点的局域网端口到带以太网端口的计算机拉一根交叉线。交叉线在电缆连接器上交换针口，这样每个终端的设备都可在正确的针口上发送和接收数据。将这种电缆放到适当的位置，您就可以以默认的 IP 地址来使用浏览器来打开实用程序。如果您有适合的电缆线(标准的以太网电缆并不能达到目的)，这种方法就会很容易，但它会迫使您断开接入点与网络的连接。

记住，一个局域网只能有一个 DHCP 服务器，这一点非常重要。如果一个局域网包含另一个可以分配数字地址的 DHCP 服务器，最好将接入点中的 DHCP 功能禁用，允许主服务器处理整个网络的地址分配，包括有线或无线节点。

这个示例说明的是，关于这个问题的一般性描述并不比特殊接入点提供的特定过程更有用。硬件手册应该包含一些安装指南，其内容涵盖了接入点的配置实用程序和适用于每个网络客户机的 Windows 网络设置。找到该手册，尽可能按照这些指南做。如果您已经将能够运行的接入点配置设置和 Windows 网络设置结合在一起(这种结合确实存在，但不是非常安全)，在纸上记下这些设置，然后保存到手册里。稍后您将会使用这些设置将更多计算机和接入点添加到同一网络中。

3.4.4　通过串行端口配置接入点

大部分接入点都包含一个串行端口，这个端口可接受一个来自远程终端(或更可能来自一个运行终端仿真程序的计算机，如 Windows 提供的超级终端程序 HyperTerminal)的直接连接。这也提供了一种区别于基于 Web 的通用配置实用程序的方法。

接入点的串行端口应该是有 9 个针口的 DB-9 数据连接器或是 RJ-45 连接器，RJ-45 看起来像是原先用于单线电话的 RJ-11 连接器的稍胖版本。如果接入点使用的是 RJ-45，制造商应该还提供了一根电缆和适配器。如果连接器是 DB-9 型，应该也有一个能直接连接到计算机 COM 端口的电缆。如果接入点需要一根 NULL 调制解调器电缆，那么在手册中应该提到关于这方面的内容。

至少一个接入点有一个 DB-9 连接器，但不能通过它直接连接到配置实用程序。D-Link 的 DI-713 无线网关有一个连接调制解调器和拨号电话线的串行端口，它可作为 WAN 连接的可选方法。

为了能通过串行端口将命令发送到接入点，可执行以下几个步骤：

(1) 在接入点和一个计算机 COM 端口之间拉一根电缆。

(2) 启动终端仿真程序，例如 Windows 提供的 HyperTerminal，然后通过连接到接

入点的 COM 端口进行连接配置。

(3) 打开接入点的连接。

(4) 如果接入点还没有打开，请打开它。您会在终端仿真程序里看到一些起始消息，如图 3-10 所示。

图 3-10　某个接入点的控制台程序或许会在设备刚启动时显示一些起始消息

(5) 当接入点准备好接收命令时，它会显示一个提示。为了确定终端仿真器正在运行，可以按 Enter 键。接入点会在一个新行中显示另外一些提示。

这时，接入点已经准备好接收配置命令。每个品牌的接入点都使用不同的命令语言，所以您不得不从手册中查找一些您必须用来改变网络设置的命令。

3.4.5　配置命令和设置

每个配置实用程序处理配置命令和设置的方式都不相同，但每个接入点都遵循同样的 802.11b 规范，它们应该包括一些相同的基本选项。当设置网络时，或许需要改变一些选项的默认值。

许多基于 Web 的配置实用程序使用选项卡或菜单来将选项列表分成几个屏幕。如果一个特殊的命令的位置没有出现在第一级屏幕上，您可以打开下一级屏幕，直到发现它，或者也可以在接入点手册中找到您所需要查看的特定导航说明。

在手册中应该描述了通过接入点的串行口改变配置的命令语言。多数情况下，一个帮助命令可以将其他命令的正确语法在计算机上显示出来。

通常，配置实用程序还会有下面几个选项：IP 地址、子网掩码、无线网络 ID、频道、安全和 DHCP。

1. IP 地址

IP 地址栏显示接入点当前正在使用的数字 IP 地址。它可能是出厂的默认设置，也就是局域网的 DHCP 服务器自动分配给接入点的地址，也可能是网管手工设置的地址。

2. 子网掩码

子网掩码标识包含接入点和通过接入点连接到局域网的无线客户机的子网。子网的地址由网管来分配。如果您的局域网没有包含子网，那么可以使用默认值 255.255.255.0。

3. 无线网络 ID

SSID(Service Set Identification，服务集标识)是包含这个接入点的无线网络的名称。当无线客户机试图连接到网络时，它会寻找某个接入点，该接入点的 SSID 和自身配置设置中的 SSID 相同。如果发现一个不同 SSID 的信号，它会拒绝连接，然后继续寻找正确的 SSID。

因此，SSID 可以有两个目的：它可以作为抵御未授权用户访问的第一条防线，而且在一个有多个无线局域网工作的环境里，它可以使每个客户机与正确的网络相连。然而，SSID 本身并不是一个特别有效的安全工具，因为有些网络适配器可以接受 ANY(任意)的 SSID，这样它会允许客户机与第一个被寻找到的接入点连接，而不用去管接入点的 SSID。

4. 频道

频道设置就是接入点与无线局域网上的客户机设备交换数据所使用的无线电频道。每个接入点在一个单一的频道上工作，但多数网络适配器搜索所有的频道来找到有相同 SSID 的最佳信号源。如果网络客户机包含扫描功能，可以假定附近的客户机设备可以找到您的接入点，而不用管频道的设定值。当您网络里的一个用户试图使用一个预设好频道的网络适配器时，接入点和客户机的频道设置就必须要匹配。

在一个嘈杂的环境里，有些频道可能会比其他频道的性能要好，因为其他网络和 2.4GHz 设备在一些频率上可能产生干扰，而在其他频率上则不会。如果附近还有其他无线网络在工作，您可以使用没有重叠的频道号，这样可以减少干扰和提高网络性能。如果还不行，就尽可能使用离得较远的频道。

如果您的网络包含多个接入点，您应该将邻近的接入点设为不同的频道。为了避免信号之间的重叠，记住使用至少分开 5 个数字的频道，如频道 1、6 和 11。

5. 安全

WEP 是一个可以防止没有正确电子密钥码的用户进入您网络的安全方案。本书第 14 章还会讲到，WEP 加密并不能有效对付蓄意的偷听者，但有总比没有好。所有的 802.11b 硬件都会支持可选的 WEP 选项，因此您必须知道如何使用它。

每个接入点都能使用 64 位 WEP 加密密钥来限制未授权的访问，而有些则会提供 64 位或更安全的 128 位两种密钥。因为 64 位密钥实际上由 40 位密钥和 24 位的初始向量字符串组成，有些程序称其为 40 位的密钥。使用 40 位 WEP 加密的接入点和网络适配器能与使用 64 位加密的设备完全兼容。

不过，有些厂家需要一个字符和数字组成的字符串作为 WEP 密钥，而其他则需要十六进制组成的字符串，或者是五组的两位数字，又或者是一个十位数字的字符串。而其他的则会向您询问密码，然后自动生成为十六进制的密钥。

通常设置禁用加密的无线网络很容易，但当您开始通过网络发送数据时，最好还是打开它。各接入点的配置实用程序中的 WEP 密钥和其他连接到接入点的所有客户机设备的 WEP 密钥都必须一样。

6. DHCP

前面“DHCP 和其他问题”一节里提及，接入点可以作为 DHCP 服务器来自动为网络里的无线客户机分配 IP 地址。

记住，同一时间内网络中只能有一个 DHCP 服务器可以被激活，如果网络里已经有一个活动的 DHCP 服务器，接入点的 DHCP 功能就必须被禁用。如果您的网络里包含多个接入点，DHCP 服务器必须只能在其中的一个中被激活，而且必须没有其他任何活动的 DHCP 服务器。

当接入点的 DHCP 服务器处于激活状态，配置实用程序会在一个屏幕上显示出当前被激活的 DHCP 客户机列表，同时还提供了启用和禁用选项，也可以是在不同窗口或屏幕里显示上述信息。

7. 其他设置

除了上面提到的一些设置之外，在接入点的配置实用程序里还有其他选项。有些选项控制嵌入到相同设备里的非无线功能，而其他的选项则允许用户指定一些可能会被客户机设备修改的任意值。

接入点手册中应该会告诉您如何设置这些值。当一个设置的意图不是很明显时，或者如果它看起来对您的网络没什么作用时，最安全的方法就是接受默认值。换句话说，如果有疑问，那就不用管它。

3.4.6　多个接入点

多数无线网络会使用多个接入点，将网络覆盖范围扩展到单个基站的信号范围以外。如果客户机设备从当前被激活的接入点移动到另外一个靠近的接入点，或者由于其他无线电信号的干扰而使信号质量下降，原来的接入点会断开链接，然后连接到正

在接收来自于客户机的最佳信号的接入点。这个技术与蜂窝电话进行漫游时不用中断通话的技术相似。

802.11b 规范允许客户机设备在网络的接入点之间移动链接，但它并没有解释如何中断一个连接。在没有标准的情况下，每个接入点的生产商都会有自己的方法，而这些方法就有可能和其他的系统不兼容。在某些方面可能会有所改变，但是在可预见的将来，您的网络中将只使用同一型号的接入点。兼容 Wi-Fi 的网络适配器将能和任意品牌的接入点一起使用，但要使两个不同类型的接入点一起工作就不安全了。

在安装有多个接入点的无线网络时，可以简易地将所有的接入点都连接到相同的有线以太网络中，然后将它们配置成处理相同的 SSID 和 WEP 密钥。如果您不能使用自动分配 IP 地址的 DHCP 服务器，那就给每个接入点分配一个不同的数字 IP 地址，但一定要在整个网络里使用相同的子网掩码和网关地址。如果接入点能作为 DHCP 服务器，记住禁用网络里所有其他接入点的 DHCP 功能。

每个接入点都必须工作在与邻近接入点所使用的不同的频道上。如果可能，使用不会互相干扰的频道号，例如频道 1、6 和 11。在一个较大的空间里，可以尝试通过交错使用频道号来保证频道能被完全分开，如图 3-11 的排列一样。

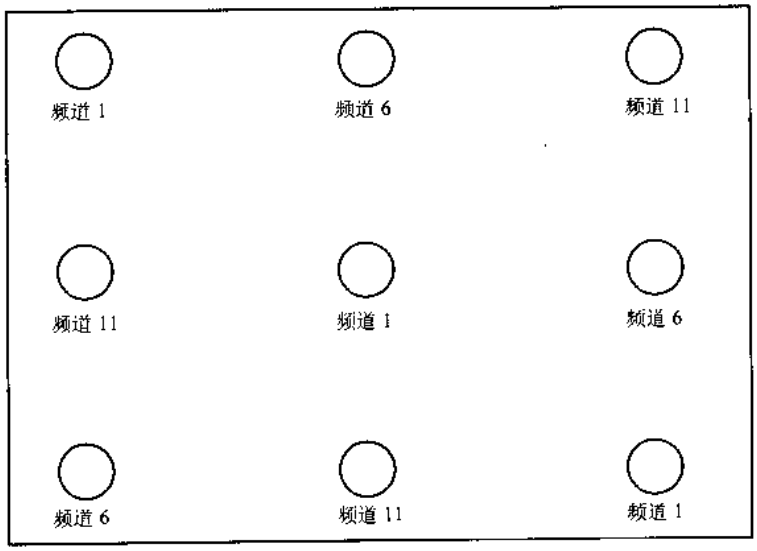

图 3-11　在一个有多个基站的网络里，将重叠的接入点相互分开

3.4.7　与集线器和网关路由器组合的接入点

多数厂家都提供将无线接入点功能与网络集线器、交换机或路由器整合在一起的产品。其他组合产品包括带有网络打印机服务器或宽带(电缆或 DSL)Internet 接入的接入点。一个整合过的产品对于一个新的小型网络，或者是为了将所有有线和无线客户机

连接到现有网络，都可以是很好的起点。因为一个整合的设备不需要分开的电源供应、外包装和每个功能的互连电缆，花费就相应比分开的组件(做同样工作)加起来要便宜。减少将所有东西连接在一起的电缆线的数量也很不错，特别是对于一个不用将所有东西都接到接线柜的小型网络而言。

为了确定这些整合设备是否是能满足您的任务需求的最好方法，可以首先确定那些需求，然后看一些不同厂家的产品目录，到网站上找到与您的需要最接近的产品。像D-Link、Linksys、Intel、Buffalo等厂家都提供了大量整合很多其他功能的接入点。

安装整合过的接入点不会与单机接入点有很大不同。每个设备都会提供一个专用配置程序，用来设定诸如接入点的工作频道、SSID和其他设置，另外还有能设置这个设备额外功能的配置选项。再提醒一下，每个产品附带的手册是能找到一些用于完成配置和安装程序的特定信息的惟一地方。

在大多数Wi-Fi网络中，接入点在日常工作中几乎是不可见的。它们被放置在橱柜上，或者放在桌子后的地板上，它们在这儿负责客户计算机和有线网络之间数据的传输。一旦您开启网络接入点并使它运行起来，您可以在要改变配置之前再关注它。

第4章　安装和配置网络接口

通常，安装一个无线网络适配器要比安装接入点要简单得多，因为多数网络适配器是即插即用的设备。不管物理配置如何，每个网络适配器都需要一个能充当适配器和计算机操作系统之间软件接口的设备驱动程序，另外还需要一个允许用户设置适配器的操作参数的配置实用程序。

4.1　安装 PC Card 适配器

PC Card 上的网络适配器可以插入到便携式计算机的 PCMCIA 槽中，或是适合于台式机扩展槽的槽适配器中(这也就意味着一种适配器可以插入到另一种适配器中)。安装 PC Card 时，您只需轻轻地将它牢固地插入槽里。当它被正确地放置后，您应该能感觉到槽中的针脚能与卡边缘的洞正好相配。

多数无线 PC Card 适配器有一个展开后能超出 PCMCIA 槽外边缘大约 1 英寸的内置天线。然而，有些适配器会带有外置天线的连接器。如果您正在使用一个外置天线，那么就将天线放在您需要进行操作的位置，然后从天线到网络适配器天线连接器拉一根天线电缆。

4.2　安装 USB 适配器

多数 USB 无线适配器都是带有内置天线的紧凑设备。由于适配器和计算机之间通过电缆连接，在你选择的第一个位置无法从接入点检测到很好信号时，可以很容易地对适配器作调整。

按照下面的步骤安装 USB 适配器：

(1) 从计算机拉一根 USB 电缆到您计划放置适配器的位置。注意 USB 电缆的两头是不同类型的连接器，因此要确保电缆计算机端的连接器要与计算机的 USB 端口相配。

(2) 将电缆插入计算机的 USB 端口。

(3) 将另一头插入到网络适配器中。

(4) 运行适配器自带的配置程序，或者使用 Windows XP 自带的无线配置工具。

(5) 打开信号强度和信号质量显示窗口。

(6) 如果信号质量不好或不是很好，调节适配器的位置来优化性能。

4.3　安装内置适配器

在台式机里添加内置适配器要复杂点，这是因为要打开机箱，然后才能将适配器插入扩展槽内。但与其他扩展卡的安装方法一样，它需要网管和比较严谨的家庭计算机用户做过这方面的工作，而不只是心里想想就行。

安装过程是这样的：拔掉电源线。打开机箱。找到一个空的扩展插槽。移开后面的金属挡板。将适配器插入插槽里，拧紧它，关机箱，插上电源，涂肥皂，洗手，重新来过，直到您累了就停止。

大部分内置适配器实际上都是有 PCMCIA 插槽(能插入扩展槽的)的 PC 卡适配器。除非适配器的手册告诉您，否则最好在您将插槽安装到计算机前将 PC 卡从槽中移开。通常要花点功夫才能将适配器准确地放进插槽内，卡尚未就位，插槽将更为灵活。在您重新装好计算机，并确信 Windows(或其他操作系统)能识别 PCMCIA 插槽后，将适配器插入槽中并加载无线适配器驱动程序。

多数内置网络适配器并不是 PCI 桥接器的真正 PCMCIA，但却使用一个更简单且便宜的 PLX 方法。这也就是说，尽管任何 PCMCIA 卡能匹配 PCI 适配器，如果没有专门的驱动程序，它们不能工作。

4.4　加载驱动程序软件

不管它们的外观如何，几乎所有的无线适配器都是即插即用型设备，这也就意味着一旦您安装好它，Windows 能自动识别到适配器。然而，在使用适配器收发数据之前，操作系统仍然需要为每个适配器加载一个特定的驱动程序软件。

驱动程序的来源很多——Windows 会自带一些驱动程序，适配器的软盘和光盘上可提供驱动程序，公司的技术支持 Web 站点上也会有相应的驱动程序。通常最新的驱动程序可以从公司的网站上找到。包含有无线适配器的驱动程序盘或下载还包括适配器的配置实用程序。这样您就可以在物理安装或连接适配器之前加载驱动程序和配置软件。

当您第一次将 PC Card 插入 PCMCIA 插槽，或是将 USB 适配器插入计算机的 USB 端口时，Windows 会检测到适配器，并且运行 Add New Hardware Wizard，如图 4-1 所示。假定您已经加载了最新的驱动和配置实用程序，那么选择自动查找选项。Windows 会找到并安装驱动程序。

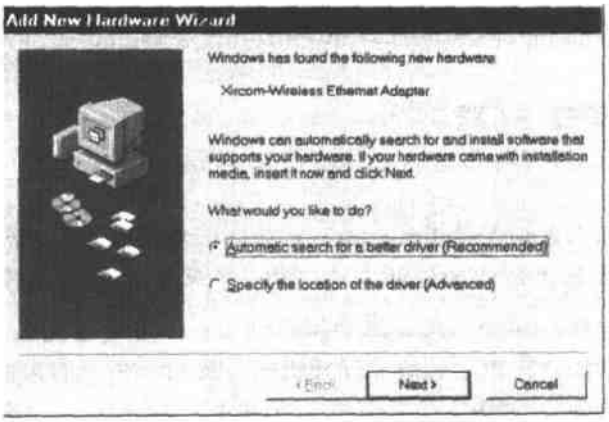

图 4-1　在第一次检测到新硬件时，Windows 用于加载驱动程序的窗口

在安装完驱动程序之后，Windows 会指导您重新启动计算机。有些配置实用程序会不管无线适配器是否被激活就自动运行；其他的则会要求用户从 Start | Program 菜单里启动程序，或是选择桌面上一个运行程序的图标。如果配置程序没有在程序窗口中打开，那它就会以一个状态图标的方式显示在系统面板里，挨着时钟显示。

Apple AirPort 的驱动程序在 Macintosh 上作为安装包一部分进行加载。在 Linux 和 Unix 系统里，您必须手动安装驱动程序。第 7 和 8 章将详细描述 Linux 和 Unix 的驱动程序。

4.5　使用配置实用程序

每个无线接入点的生产厂家都会使用不同的配置实用程序，对这一点不用感到奇怪。它们控制相同的设置和选项，都显示类似的内容，但多数公司都宁愿发布自己的软件，而不是许可别人已有的程序。其中有一些例外，但多数情况下，每个品牌的适配器都会有一个不同的实用程序。

配置实用程序的最主要不同点是关于选项和状态信息的布局，而不是程序的功能有什么不同。有些厂家使用一个程序显示无线链接的当前状态，使用另一个程序来改变配置设置，而其他厂家使用单个程序(带有独立的选项卡或菜单选项)来显示状态和配置信息。从实际用途来看，每个配置实用程序都是一样的。

一些配置实用程序会随 Windows 启动而自动运行，这对一直使用无线链接的计算机来说很好。然而，在不经常使用活动网络连接的移动计算机上，加载配置实用程序只会增加启动计算机所需的时间，而且会浪费一些系统资源。为了避免配置程序在 Windows 98、Windows ME、Windows XP 系统上自动运行，可以在 Start | Program | Startup 菜单或 msconfig 程序中标识并禁用自动运行的程序。

4.5.1　Microsoft 无线网络连接实用程序

Windows XP 包含支持绝大多数无线网络适配器的无线网络连接实用程序。当 Windows 支持无线适配器时，它会自动运行无线网络连接实用程序，除非您在 Wireless Network Connection Properties 窗口中的 Wireless Networks 选项卡中禁用它，如图 4-2 所示。如果 Windows 实用程序不支持适配器，它会使用适配器所提供的配置实用程序。

如果您正在 Windows XP 中使用 Orinoco 适配器，生产商建议您使用 Microsoft 的实用程序，而不是 Orinoco Client Manager。实际上，无论使用哪一种，不会有很大区别——它们都显示选择一个适配器需要的信息，并且提供类似的控制。您应该尝试这两个程序，然后选择一个较容易使用的。其他厂家的适配器也一样，因为 Microsoft 和适配器厂家扩展了 Wireless Network Connection 实用程序来支持附加的适配器。

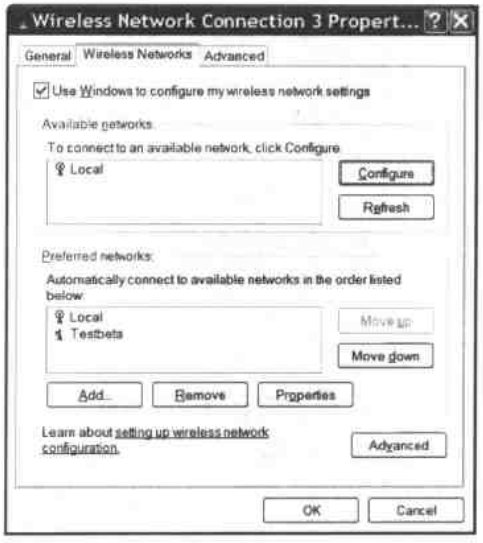

图 4-2　在 Properties 窗口中使用 Wireless Networks 选项卡来启用/禁用 Wireless Network Connection 实用程序

4.5.2　读取状态信息

图 4-3、4-4 和 4-5 分别显示了两个不同品牌的无线适配器状态。图 4-6 是 Windows 的 Wireless Network Connection 状态显示。

每个程序都提供了一组不同信息。大多数状态显示包括下面几项：

- **信号强度**　信号强度是最新扫描期间适配器所收到的无线电信号的功率数值。绝大部分程序使用百分比来显示信号强度，但有些也使用 dBm(毫瓦分贝)来显示测量到的强度。实际上，信号强度值在测量信号随地点改变而变化时非常有用，但在不同厂家的产品之间就没有什么参考价值了。
- **信号质量**　信号质量就是在最近扫描过程中适配器接收到的数据信息包的质量。

100%则表示所收到的所有数据信息包都很好。

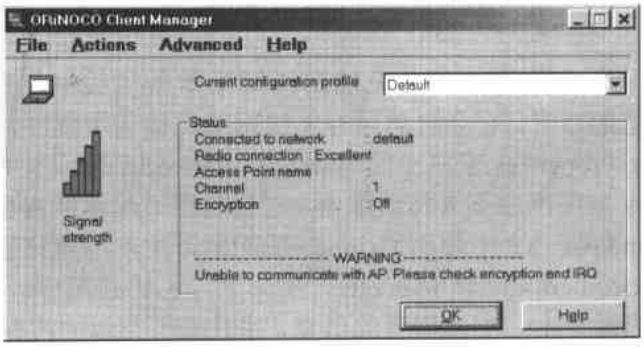

图 4-3　Lucent 的 Orinoco Client Manager 显示了与 Wireless Network Connection 实用程序相同的信息，但使用不同的窗口布局

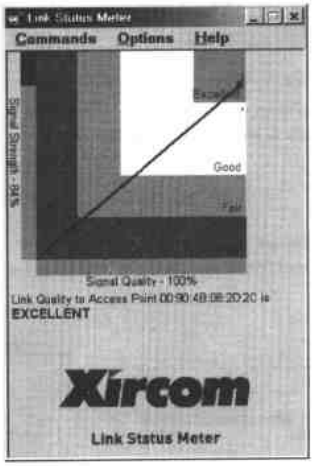

图 4-4　Xircom(和 Cisco)分别显示信号强度和其他状态信息

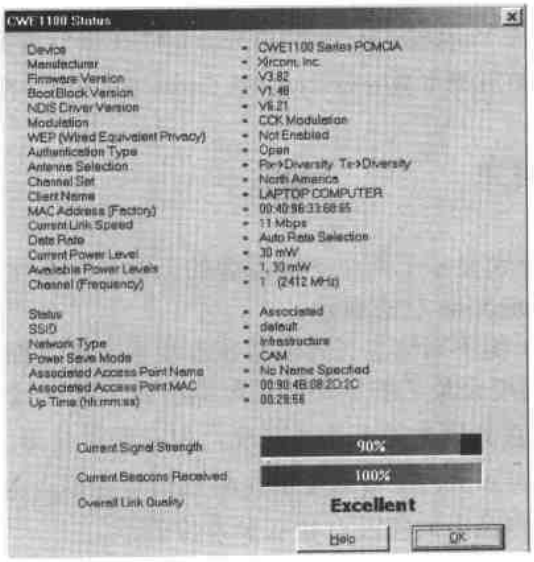

图 4-5　Xircom 的 Status 窗口比其他厂家的提供更多信息

图 4-6　Windows XP 中的 Wireless Network Connection 窗口用另一格式显示相同信息

- **总体质量**　总体质量是一个基于信号强度和信号质量而计算出的数值。它通常可用 Excellent、Good、Fair 和 Poor 来表示。
- **链接速度或数据率**　链接速度就是适配器和当前使用的关联接入点之间理论上的数据传输速度。
- **关联**　这个字段确认适配器已经和有线 LAN 建立了连接。
- **MAC**　这个字段标识指适配器惟一的 MAC 地址。
- **SSID**　SSID 是设备当前连接的局域网名称。无线局域网上的所有节点和接入点都必须用同一 SSID。
- **网络类型**　如果网络使用多个接入点，网络类型就是基础网络。如果是对等网络，那就是特别网络。
- **频道**　该字段显示了适配器正在使用的无线电频道。
- **加密**　这个字段显示了适配器当前是否在使用 WEP 加密，以及使用哪种加密方式(如果适配能处理 64 位和 128 位的加密方式)。
- **活动**　该字段显示了适配器已发送和接收的数据包数量。

4.5.3　无线配置工具

配置工具是设置或改变您的适配器用于和网络进行通信的本地设置的地方。有些实用程序在一个窗口显示状态信息，在另一窗口改变设置。

网络类型、SSID 和 WEP 加密密钥对网络中每个节点都必须一样。网络中每个适配器的数字 IP 地址必须惟一，但子网地址都必须一样。

如果您的适配器不能自动扫描活动频道，或是这个区域内有很多接入点，您必须用配置工具来设定最近的网络接入点所使用频道的频道号。

设置一个充满适配器的网络的最简单方法就是先从配置接入点开始，然后注意无线配置，您必须在单个适配器里与它相匹配。如果您希望您的用户配置他们自己的适配器，您将需要准备一个标准信息栏或卡片来列出这些设置：

- 网络的 SSID
- 网络类型(基础或特别网络)
- DHCP 开启或关闭
- 分配给适配器的 IP 地址和子网掩码(若 DHCP 关闭)
- WEP 加密类型(无、40/64 位或 128 位)
- WEP 加密密钥(或者可提供它的 help desk 的电话号码)
- 频道号
- 前导长度
- 访问网络的 URL、登录名和密码(如果需要的话)

无论您对上面这些说明有多了解，如果没有帮助，一些人在连接到网络时肯定会遇到麻烦。因此，表中应该包含一些能在安装适配器和配置过程中给予帮助和详细讲解的人的电话或名称。

如果您的大多数用户都使用同样的适配器，您可能就需要一些关于适配器配置窗口和 Windows Network Settings 窗口的快照，逐步指导打开那些窗口。

4.5.4 从一个网络移到另一个网络

如果您在多个无线网络里使用便携式计算机，您或许需要准备一份小抄，在其中写上如何配置您的网络适配器，从而使其能在您经常使用的网络中工作：家庭、办公室、咖啡店和飞机场等地方。有些配置程序会提供两到多个预设的配置文件，但如果没有的话，您就必须在移动到另一个网络时设置所有选项。

Windows XP 中的 Wireless Network Connection 实用程序有一个自动无线配置特性，它可以检测在范围内所有网络，然后自动配置您的无线适配器。如果您的适配器能与 Windows 实用程序兼容，这将会减少很多时间和精力。然而，如果 Windows 不能检测到应该在某个位置的网络，这就要您使用一些嗅探工具如 Network Stumbler 来自己搜索。

可以按照下面的步骤来使用 Windows XP 的自动无线配置特性：

(1) 单击 System Tray 上靠近时钟标志的网络图标，从而打开 Wireless Network Properties 窗口，或打开 Start | Settings | Network Connections，右击无线网络连接的图标，从弹出的菜单中选择 Properties。

(2) 选择 Wireless Networks 选项卡。

(3) 通过选择 Use Windows to Configure My Wireless Network Settings 选项来启用

或禁用自动配置。

(4) 单击 Advanced 按钮打开一个窗口，其中可以设置 Windows 将自动检测到的网络类型。图 4-7 所示为一个 Advanced 窗口。

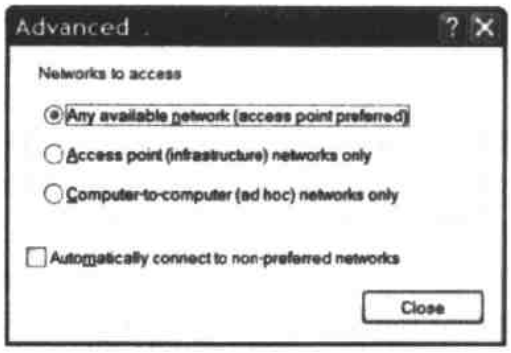

图 4-7　高级无线网络连接属性窗口可用于指定 Windows 将自动检测的网络

(5) 选择您的计算机需要检测的网络类型。为了指导 Windows 检测和连接到附近的网络，即使它不在 Preferred Networks 列表中，您仍然需要打开 Automatically Connect to Non-preferred Networks 选项。

4.6　超越 Windows

每个适配器生产商都为大多数流行的 Microsoft Windows 版本提供软件，但它们并不是您使用无线适配器的惟一操作系统——如果您可以找到合适的驱动程序。一些不常见的操作系统的驱动程序应该能在适配器生产厂家的技术支持 Web 站点或是致力于该操作系统的用户讨论组中找到。

对于 Macintosh 用户而言，最佳选择就是使用 Apple 的 AirPort 适配器和它所提供的软件，它们与其他的 802.11b 网络完全兼容。然而，也有其他一些适配器，只要找到合适的驱动程序，它们也能工作在 Macintosh 系统下。Apple 的 AirPort 适配器是 Orinoco 产品的私人版本，因此您可以用 Apple 的程序来驱动 Orinoco 适配器。第 6 章会提到如何在 Macintosh 系统里使用 AirPort 的软件。

如果您手上还有其他一些品牌的 PC Card 或 USB 无线适配器，那么也不要放弃希望。Cisco 和其他一些厂家也提供 Mac OS 的驱动程序和配置软件。可以到适配器厂家的 Web 站点上寻找最新版本。

有些适配器的驱动程序也能用在 Linux、FreeBSD、NetBSD 等其他类型的 Unix 系统上，有些直接来自厂家(例如 Orinoco 和 Cisco 通过 Web 站点提供 Linux 的驱动程序)，有些则来自用户组。一些较流行的最新 Unix 和 Linux 版本都包含多种 802.11b 芯片组

的驱动程序。第 7 章和第 8 章有关于如何在无线以太网络中使用 Unix 和 Linux 的更详细内容。

4.7 信号强度和信号质量

多数无线实用程序使用条形图或百分值显示信号强度和质量，但它并没有告诉您100%的信号质量指的是什么的百分之百。要注意信号强度和信号质量并不是一回事，这一点相当重要；无线适配器可以不用接收“满强度”的接收信号就能以最快速度传输数据。只要接收器能接收到一个清晰的信号，网络的性能就能够接受。如果接收器受到来自其他无线网络或使用相同无线电频率的设备(如无绳电话和微波炉)的干扰，那么即使是很强的信号也不能保证网络的性能。

即使数据传输速率比最快速率要慢，它也不会有什么不同。例如，如果您正使用 Wi-Fi 网络通过 DSL 线路(速度大约在 5Mb/s)将计算机连接到 Internet，即使您的本地网络速度从 11 Mb/s 降到 2 Mb/s，这也不会产生什么影响；因为该速度仍然是您可以承受的宽带速度。

用在 Wi-Fi 网络的扩频无线电信号与 FM 调频无线电信号不太一样，但干扰和信号质量问题是类似的。如果您居住在或靠近一个大城市，您或许可以用厨房里的无线电接收到很多 FM 电台。有些电台的发射台比较靠近您家，但有的可能离您家很远。但只要您的收音机能接收到最小可用级别的信号，收音机就能完美地将音乐播放出来；只要你的无线电能收到最低可用级别的电台，一英里外大学里的小电台的信号质量就能和大商业电台(在山上安装了更为强大的发射器)的一样好(这只是技术上的讨论——编程的质量就是另外一件事了)。另一个方面，如果您处在电台覆盖区域的边缘，或是附近有使用相同频率的电台，您想收听的电台的播音就会显得很嘈杂，而且很难听明白。同样，无线网络链接的整体质量也受到信号强度和多余干扰存在与否的影响。

对信息频道内噪声的技术定义是指“任何多余的能量或信息”。您需要您的适配器接收的惟一东西就是来自您自己网络接入点的数字信号，其他在接收器里出现的东西都是噪声。这包括来自其他无线数据网络、其他使用相同频率的无线电和来自然界(如闪电)的干扰。总结为一点就是，802.11b 网络中用到的数字技术和扩频无线电系统能很好地屏蔽干扰，但当噪声与你想要的信号的强度相同时，网络就会进行错误校验，直到它能确保一个可以识别的信号从发射器传到接收器。

噪声流或其他尝试在同一时间使用相同频道的无线电会减慢链路的数据传输速率，因此一个弱信号也能做到这一点。如果发射器和接收器之间的距离增加，接收器检测到的能量会降低，甚至低到接收器无法对数据解码。如果在这两个设备之间存在吸收辐射能量的物理阻碍，那么有用的信号覆盖区域就会更少。您可以用高增益天线来增

加信号强度，并且应该将天线架到塔顶或建筑物的顶端来增加信号能到达的距离，但有时信号强度减弱到无法使用。

如果确实发生了信号减弱的问题，您可以使用信号质量和强度测量工具来帮助您找到问题所在：如果信号很强但质量很差，大概是由于某种干扰的影响；如果信号质量和强度都很低，这可能是由于您离接入点太远，或是存在阻碍物。如果网络不能成功地传输数据包，接收器端的设备会指示发射设备重新发送一次数据包。这可能是由于链接(无线电或有线)中存在干扰或噪声，也可能是由于其他用户想同时使用相同频道，或者可能是无线电信号对于接收器来说太弱，以至于不能对包中的数据进行解码。数据流中的一到两个重复数据包不会造成什么麻烦，但如果在接收器接收数据之前将数据包发送多次，实际的数据传输速度就会比理论上的速度的一半还要少。一对 802.11b 无线电设备会通过降低传输速度来对弱信号进行补偿(这与嘈杂电话线路里解决说话慢和重音等问题的方法相同)，但效果是一样的：接收数据的时间会相应增加。

慢的数据传输并不都是由网络的无线电部分造成；如果网络通信量很大，或者网络的有线部分里有某种噪声，这些都会降低传输速度，因此很多问题都会导致这一相同后果。如果数据传输速度已经降低，原因可能就出在无线电链接或服务器，或者是网络中的其他部分上。为了避免这一问题，您可以在一个客户计算机上运行配置实用程序或状态报告程序。如果信号强度低，可尝试移到其他位置，远离您的计算机和接入点之间的障碍物；如果信号强度较高而质量差，网络适配器可能在接收网络数据的同时接收了噪声；如果两者都很好，但就是网速很慢，这可能是服务器或是网络其他地方的原因。

第5章　Windows下的Wi-Fi

在理想的网络世界中，可以将无线网络适配器插入计算机，然后启动它，并且立即连接到网络上。这一切都不麻烦。当 Windows 在启动期间检测到网络适配器时，它会自动在桌面上放置一个网络图标，并配置一组标准网络资源。

遗憾的是，任何一件事都不是那么简单的。在开始通过无线网络传输数据之前，您将必须告诉Windows如何和在哪儿找到网络，以及如何通过无线局域网连接到Internet。本章将详细解释使 Windows 和无线局域网一起工作的通用原理，以及您必须在不同 Windows 版本下配置网络工具和特性等特定过程。这也许很乏味，但如果您没有正确完成，网络就不能正常工作。

在 Windows XP 中，如果您的网络适配器含有与 Microsoft 的自动配置工具相兼容的固件。多数常见品牌的适配器并没有，因此您必须手工配置无线网络连接。即使 Windows 可识别您的适配器，了解可以看到的表面现象后面发生了什么也是很有用的。

如果您实际配置过 Windows 的网络，就不会在无线网络上花太大精力。对于 Windows 来说，无线适配器只是另外一种在应用程序和操作系统之间交换数据的网络接口。一直到 Windows XP，“无线”的一些基本东西都发生在一个单独的实用程序里；在 XP 中，网络属性对话框里有一个无线专有的设置选项卡。在 Windows 中配置无线网络其实就是使被配置的计算机认识到自己被连接到网络上，然后设置一些网络服务器和服务的地址。

遗憾的是，Windows 将配置选项都分散到了虚拟映射中，这样，一系列指向所有选项的指针将对您非常有帮助。您会在本章后面学习这些内容。

5.1　常规的 Windows 网络配置

不同 Windows 版本所使用的配置工具可能不一样，但都完成同样的事情：计算机的 IP 地址，子网掩码和网关地址设置，所有这些都必须与网络其余部分所需的值相同。您可以完全不管它们是什么就进行设置，但知道一些网络实际工作方式的内容要有用得多。

5.1.1　IP 地址

一个网络客户机的数字 IP(Internet 协议)地址是一个正式的标识，相同网络里的其他计算机可以凭借它来找到这台机器。网络里的每台计算机都应该有不同的地址。

管理 Internet 的机构已经建立了一个复杂的数字系统，通过这个系统为每台连接到 Net 上的设备分配一个惟一的地址。数字 IP 地址由四组 0-255 之间的数字组成，这样整个 IP 地址的范围就是从 0.0.0.0 到 255.255.255.255。这些数字有时还可以称为“八位字节”，因为它们使用了八进制数字(二进制的 1111111 等于十进制的 255)。

一个数字 IP 地址可以标识一台计算机，或者可以是通过路由器连接到由两台或多台计算机组成的局域网的网关。如果局域网通过网关连接到 Internet 上，每个本地计算机也必须有惟一的数字 IP 地址。根据网络设计，局域网上的每台计算机可以有一个连接到 Internet 的真实地址，或者有一个在为私有用户设计的范围内的 IP 地址，并且还有一个将局域网连接到 Internet 上并在私有和公共地址之间进行转换的网关。

为了避免本地 IP 地址和 Internet 上的地址相冲突，有一些数字范围被保留为在本地网络里使用：

- 10.0.0.0~10.255.255.255
- 172.16.0.0~172.31.255.255
- 192.168.0.1~192.168.255.255

分配地址

在有些网络中，DHCP(Dynamic Host Configuration Protocol，动态主机配置协议)服务器会为网络中的每个客户机设备分配不同的 IP 地址。无论客户机何时连接到网络上，服务器都为每个客户机设备分配地址，因此相同的客户机在不同的会话中就可能有不同的地址；这就是为什么它被称为动态主机配置的原因。

DHCP 服务器通常在控制网络中所有设备的路由器里。在一个纯粹的无线网络里，它可能就在接入点中；在一个由无线和有线网络组成的混合型网络里，DHCP 服务器很有可能在 Internet 网关上。图 5-1 所示为一个典型网络中的服务器。

如果 DHCP 正处于活动状态，局域网上的所有用户应该指导 Windows(或其他网络操作系统)自动获得 IP 地址。如果网络没有使用 DHCP 服务器，网管就必须手工为每台机器设置永久 IP 地址。如果您手工分配了地址，那么就在一个文本文件里保存一个地址列表的副本，将地址列表写在纸上。

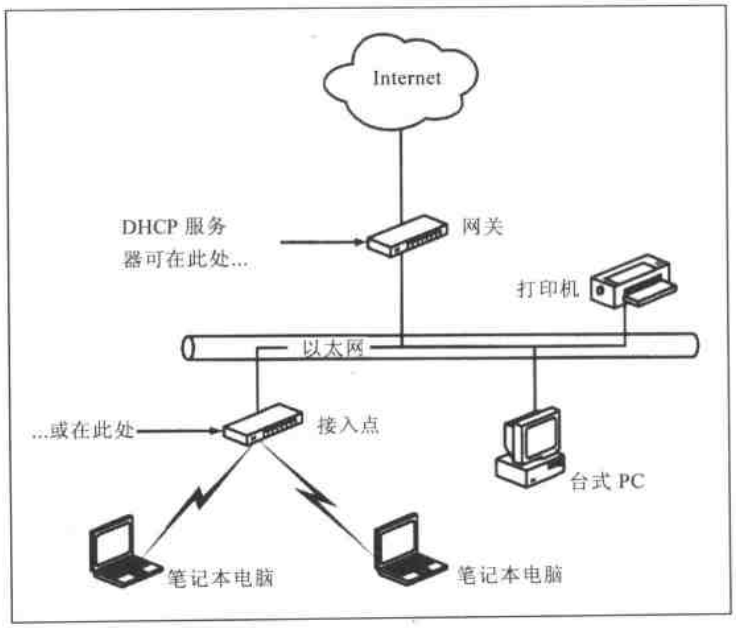

图 5-1 为局域网中所有设备分配本地 IP 地址的 DHCP 服务器

接入点的手册里应该为客户端设备的 IP 地址范围指定了默认值。如果使用 DHCP，该服务器会自动为它们分配地址。如果没有用 DHCP，您必须为网络上的每个设备设置一个该指定范围内的 IP 地址。如果您将无线网络连接到有线局域网上，必须将接入点的地址范围与局域网中的地址范围设成一样。

5.1.2 子网掩码

子网掩码是一个四组数字组成的字符串，它指定一个较大网络中的哪一部分包含计算机或其他网络节点。这四组数字的每一个通常不是 255 就是 0。这些数字指定 IP 地址的哪些部分标识网络或本地子网，以及哪些部分标识网络上单独的计算机或其他节点。例如，如果子网掩码是 255.255.255.0，那么网络里的所有数字 IP 地址都必须是 XXX.XXX.XXX.ZZZ，其中 XXX.XXX.XXX 对每个地址都相同，而 ZZZ 应该不同才行。

子网掩码对于任何接入点和这些接入点所服务的无线客户机应该都一样。在一个中小型的网络里，子网掩码通常是 255.255.255.0。

5.1.3 网关

网关指的是无线接入点、路由器或其他设备，它们充当局域网中计算机和不是本地网络一部分的其他设备或网络之间的接口。当任何一个不是本地网络中的计算机试图

与网络中的设备进行通信时，它都必须通过网关传输数据。

网关地址(有时还可以称为默认网关)是一个网关服务器的数字 IP 地址。根据无线网络设置方式，这个地址通常被分配给接入点的地址，但如果您的无线设备被配置为一个简单的网桥，那么这个网关地址就应该和您的有线网络网关相同。

如果一个接入点有集线器或路由器的双重功能，该接入点用于有线和无线客户机的网关地址应该和它用于与局域网或 Internet 服务器通信时的网关地址不同。如果您正在配置网络客户机，记住使用接入点的局域网 IP 地址作为默认网关，而不是广域网的 IP 地址。

5.1.4　DNS 服务器

DNS(Domain Name System，域名系统)服务器是一台将域名(如 nostarch.com 或 hard-cider.com)转换成使用那些地址的计算机或其他设备的数字 IP 地址。有些 DHCP 服务器自动提供一个 DNS 服务器地址，但有些则要求每个用户在客户机的 TCP/IP 配置里手工添加 DNS 服务器。如果您没有使用 DHCP，就必须至少指定一个 DNS 服务器地址。

绝大多数网络和 Internet 服务供应商会使用两个或多个 DNS 服务器，这样可以在主服务器脱机时提供一个自动备份。您的网管或 Internet 服务供应商应该向您提供网络的 DNS 服务器的地址。

有些接入点和网关也需要一个 DNS 服务器地址。接入点或网关的服务器列表应该和每台客户机的列表一样。

5.1.5　文件和打印机共享

如果文件共享被激活，其他网络用户就可以从您的计算机里读取和改写文件。打印机共享允许其他用户发送文件和文档到一个共享打印机上进行打印。在 Microsoft Networking 中，一个包含可以被其他用户使用的文件的文件夹称为共享文件夹。

共享文件或文件夹的访问级别可以指定其他用户可以读取文件但不能进行修改，或者其他用户可以添加、删除或修改文件的内容。

5.1.6　网络接口适配器选项

如果您不能在配置实用程序中找到设置或选项，那么可以查看无线适配器的 Properties 窗口。每种类型的网络接口适配器的驱动程序都会包含一些控制适配器的特

定特性的选项，例如网络中的客户机所使用的名称、数据传输速率、工作模式和省电模式。图 5-2 显示了一个典型的适配器属性列表。

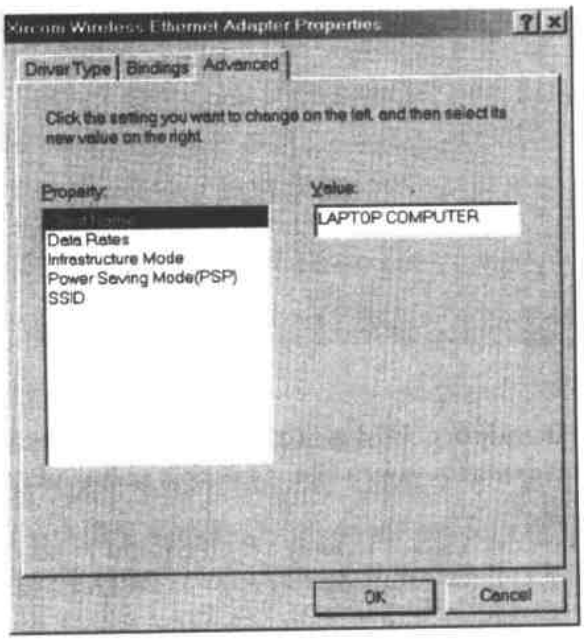

图 5-2　控制多个选项的适配器属性窗口

要打开 Properties 窗口，您可以定位到 Windows Control Panel，双击 System 图标，然后选择 Device Manager。打开 Network Adapters 列表，双击您的无线适配器的条目。选项列表就在 Advanced 选项卡下。

很多相同的适配器选项也出现在适配器自带的配置实用程序中，另外 Windows XP 的 Wireless Configuration Utility 中可能也会有。如果您在某个地方改变了一个属性，这个改变同样会在您下次打开它的另外一个位置里出现。

5.1.7　计算机命名

网络使用数字 IP 地址来查找和标识您的计算机，但网络的用户则需要使用一个比较容易识别和记住的名称，而不是一个数字和点组成的字符串。多数用户不会知道 192.168.0.34 其实是办公室里的一台计算机，而 192.168.0.37 是厨房里的一台笔记本电脑。因此您(或网管)必须为网络里的每个计算机分配一个名称。这个名称将出现在所有能通过网络访问到的计算机目录和列表中，如图 5-3 所示。每台计算机都有惟一的名称，该名称的最大长度为 15 个字符和空格。

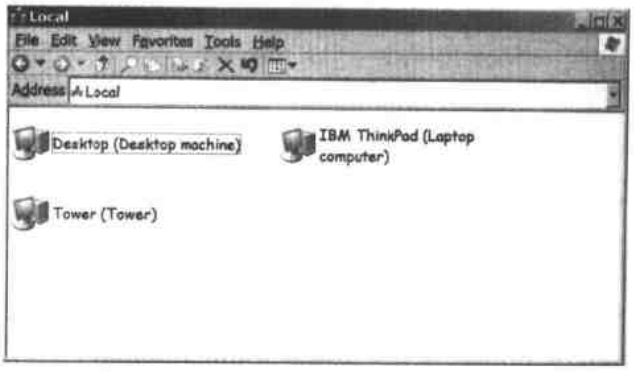

图 5-3　在一个网络窗口中显示网络上所有的计算机名称和描述

Computer Description 字段不是必须的，但它可以比仅有 15 个字符的名字更为详细地描述网络客户机的信息。

Windows 还提供一个空间将网络上的所有计算机分配到工作组中。在小型局域网中，您可能需要将所有的计算机分配到一个工作组里。因此，网络中所有计算机的 Workgroup Name 设置应该都一样。

在有些无线网络中，工作组的名称必须和接入点所用的 SSID 一样，特别是当网络配置实用程序不能显示附近网络的列表时。如果不能进行连接，可以尝试将工作组名称改成要连接的网络的 SSID。

5.2　配置 Windows 98 和 Windows ME

Windows98、Windows98 SE 和 Windows ME 都有相似的网络配置工具。

5.2.1　IP 地址和子网掩码

按照下面的步骤设置 IP 地址和子网掩码：

(1) 从 Control Panel 里双击 Network 图标。

(2) 在 Configuration 选项卡里选择您的适配器的 TCP/IP 条目，单击 Properties 按钮。

(3) 如果它不可见，单击 IP Address 标签。Properties 窗口将如图 5-4 所示。

(4) 如果网络里的接入点或其他设备的 DHCP 服务器已经开启，选择 Obtain an IP Address Automatically 选项。如果您没有使用 DHCP 服务器，选择 Specify an IP address 选项，然后在 IP Address 栏中输入分配给这台计算机的 IP 地址。

(5) Subnet Mask 栏可以在控制 IP 地址的相同 TCP/IP Properties 选项卡中找到。如果您的网络里没有使用 DHCP 服务器，输入接入点所用的子网掩码。

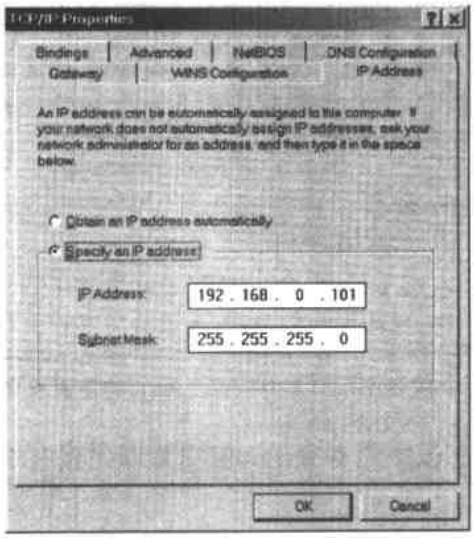

图 5-4　控制网络连接选项的 IP Address 选项卡

5.2.2　网关

按照下面步骤设置网关地址：

(1) 在用于设置 IP 地址的 TCP/IP Properties 窗口中单击 Gateway 标签，会出现如图 5-5 所示的对话框。

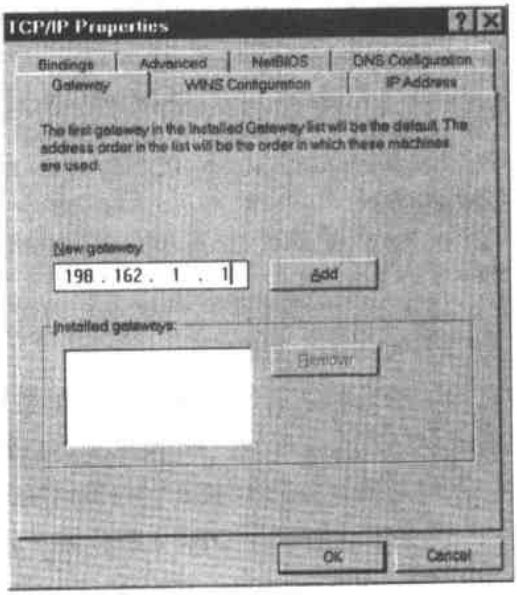

图 5-5　使用 Gateway 选项卡设置网关地址

(2) 在 New gateway 栏里输入无线接入点的局域网 IP 地址，然后单击 Add 按钮。

5.2.3　DNS 服务器

按下面的步骤配置 DNS 选项：

(1) 在 TCP/IP Properties 窗口中单击 DNS Configuration 标签，显示如图 5-6 所示的对话框。

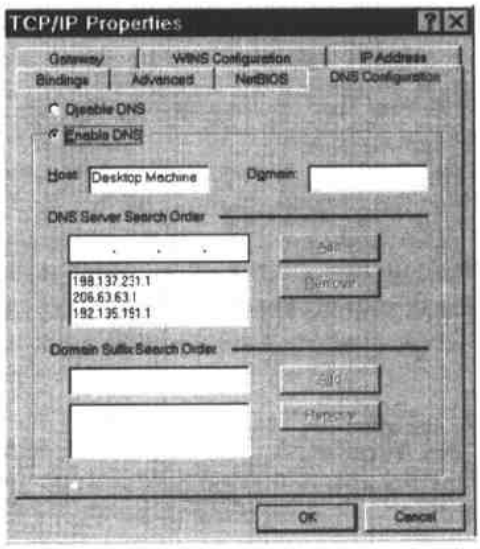

图 5-6　使用 DNS Configuration 选项卡设定命名服务器选项

(2) 如果 DHCP 服务器为网络客户机分配了 DNS 地址，选择 Disable DNS 选项。如果网络使用静态 DNS 服务器，则选择 Enable DNS 选项。

(3) 如果不可见，在 Host 栏里输入计算机的名称。

(4) 如果局域网、接入点或 DHCP 服务器使用一个域名，在 Domain 栏里输入该域名。

(5) 在 DNS Server Search Order 栏中输入您的网络所使用的每个 DNS 服务器地址，单击 Add 按钮。您的网管或 Internet 服务供应商应该为您的网络提供正确的 DNS 地址。

(6) 单击 TCP/IP Properties 窗口里的 OK 按钮，然后在 Network 窗口里保存新的配置设置。Windows 会保存这些改变，然后要求您重启计算机。当重启完毕后，新的设置将被激活。

5.2.4　文件和打印机共享

为了使其他网络用户可以使用文件夹或整个驱动器的内容，右击文件夹或驱动器的图标，然后从下拉菜单里选择 Sharing 选项。Properties 对话框如图 5-7 所示。

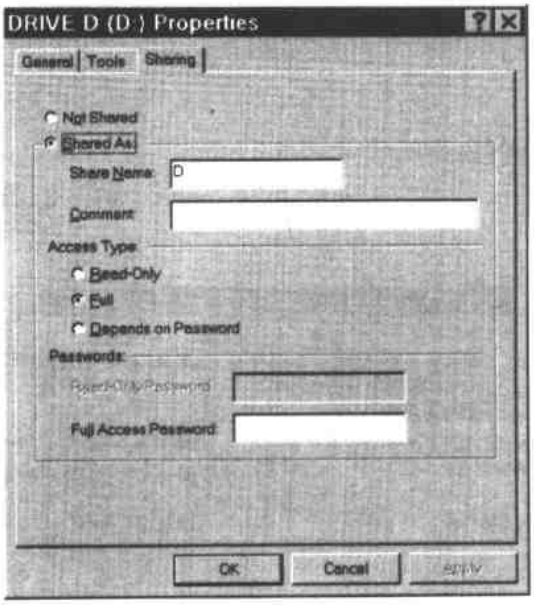

图 5-7　用 Sharing 选项卡设定文件夹或驱动器的共享特征

为了将文件夹或驱动器的访问权限制在本地计算机用户，可以选择 Not Shared 选项。要使它能被其他计算机用户使用，可以选择 Shared AS 选项，然后选择您需要为该资源提供的访问类型。

如果您已经设定一个文件夹或驱动器的共享访问属性，该文件夹或驱动器的图标会改变。如果共享被允许，一个手型图标会将这个共享元素提供给网络。

5.2.5　网络接口适配器选项

按照下面的步骤改变网络接口适配器选项：

(1) 打开 Control Panel，双击 Network 图标。Network 窗口会出现在屏幕上。

(2) 单击 Configuration 标签，可以看到一些已安装的网络组件显示在列表里。

(3) 在组件列表的最上面选择网络适配器的第一个项目，然后单击 Properties 按钮。Adapter Properties 窗口将弹出。

(4) 单击 Advanced 标签，如图 5-8 所示的属性列表将显示。

(5) 将列表中各个属性变成醒目显示，观察 Value 栏中的当前设置。有些值是文本字段，有些则是下拉式菜单。如要改变文本字段的当前值，可以选中当前文本并输入新值。要改变菜单里的值，可打开下拉式菜单并选择您想使用的新值。

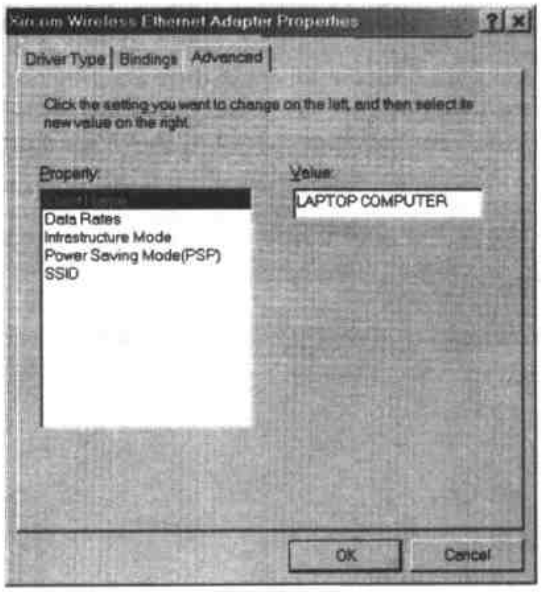

图 5-8　在 Adapter Properties 窗口中使用 Advanced 选项卡配置网络适配器

(6) 单击 OK 按钮保存改变并关闭窗口。单击 Network 窗口里的 OK 按钮回到桌面。

有些无线网络适配器，包括一些 Orinoco 产品，不接受任何选项设置。如果您在 Adapter Properties 窗口里没有看到 Advanced 选项卡，那么使用由适配器提供的配置实用程序改变适配器的设置。

5.2.6　网络标识

在连接到网络之前，必须为计算机起个名称。在 Windows 98 和 Windows ME 中，这个选项设置位于 Network 窗口的 Identification 选项卡中。按照下面的步骤改变这些设置：

(1) 打开 Control Panel，双击 Network 图标。Network 窗口出现在屏幕上。

(2) 单击 Identification 标签，会看到如图 5-9 所示的页面。

(3) 在 Computer Name 栏里输入在网络上标识您的计算机的名称。

(4) 在 Workgroup 栏里输入网络的 SSID 值。

(5) 如果您还想为其他网络用户详细描述您的计算机，可以在 Computer Description 栏里输入文本。

(6) 单击 OK 按钮保存更改，然后关闭 Network 窗口。

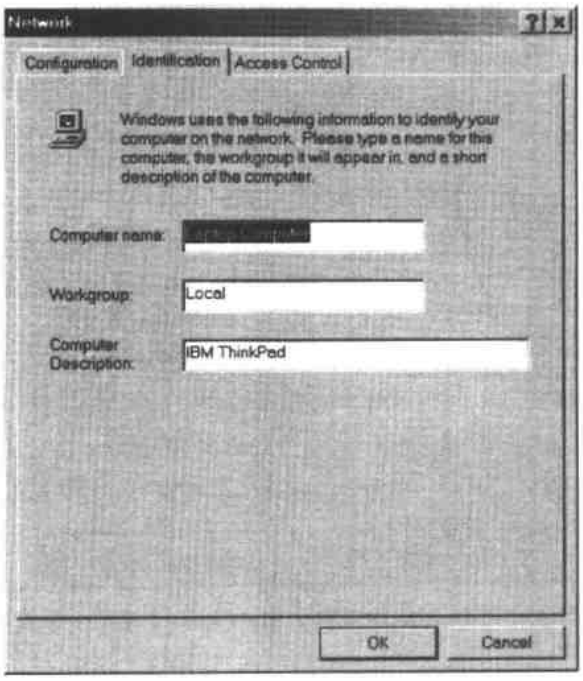

图 5-9　用 Identification 选项卡改变计算机名和网络的 SSID 值

5.3　配置 Windows 2000

Windows 2000 和 Windows 其他早期版本都有相同的配置选项，但其中有一些被放置在不同的地方。

5.3.1　IP 地址和子网掩码

按照下面的步骤设置 IP 地址和子网掩码：

(1) 打开 Control Panel，双击 Network and Dial-Up Connections 图标。带有每个网络连接配置文件图标的窗口将会出现在屏幕上。

(2) 无线以太网连接的网络连接配置文件是 Local Area Connection。右击该图标，从弹出菜单中选择 Properties。如图 5-10 所示的属性窗口将出现在屏幕上。确定您的无线网络适配器的名称出现在 Connect Using 栏中。

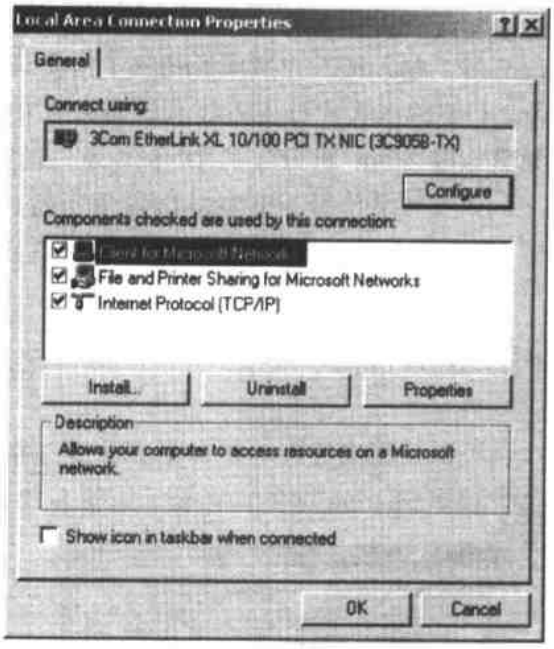

图 5-10　选择 TCP/IP 条目设置网络选项

(3) 在已安装的条目列表中选择 Internet Protocol(TCP/IP)，并单击 Properties 按钮。TCP/IP Properties 窗口将如图 5-11 所示。

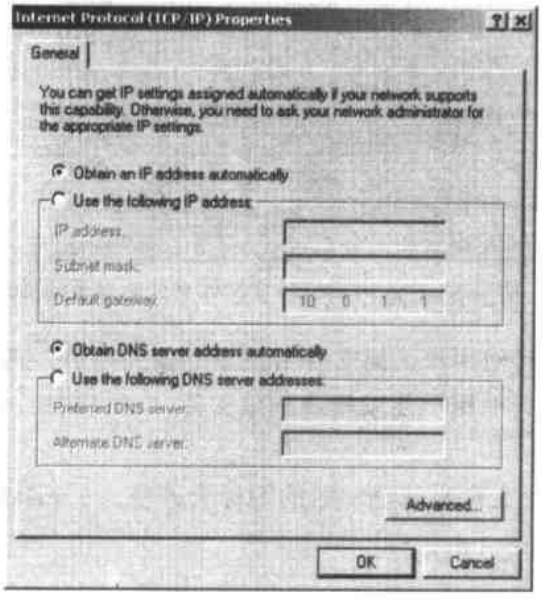

图 5-11　TCP/IP Properties 窗口控制网络连接选项

(4) 如果网络里的接入点或其他设备的 DHCP 服务器已经开启，选择 Obtain an IP Address Automatically 选项。如果您没有使用 DHCP 服务器，选择 Use the Following IP Address 选项，然后在 IP Address 栏中输入分配给这台计算机的 IP 地址。

(5) Subnet Mask 栏可以在也控制 IP 地址的 TCP/IP Preoperties 选项卡里找到。如果网络里没有使用 DHCP 服务器，输入接入点所用的同一子网掩码。

(6) 在 Default Gateway 栏里输入无线接入无线点的局域网 IP 地址。

(7) 如果 DHCP 服务器给网络客户机分配了 DNS 地址，选择 Obtain DNS Server Address Automatically 选项。如果网络使用一个静态 DNS 服务器，选择 Use the Following DNS Server Address 选项，然后输入您的网管或 Internet 服务供应商提供的 DNS 地址。

5.3.2 文件和打印机共享

为了使其他网络用户也可以使用文件夹或整个驱动器的内容，右击文件夹或驱动器的图标，并且从弹出菜单中选择 Sharing 选项，将显示如图 5-12 所示的对话框。

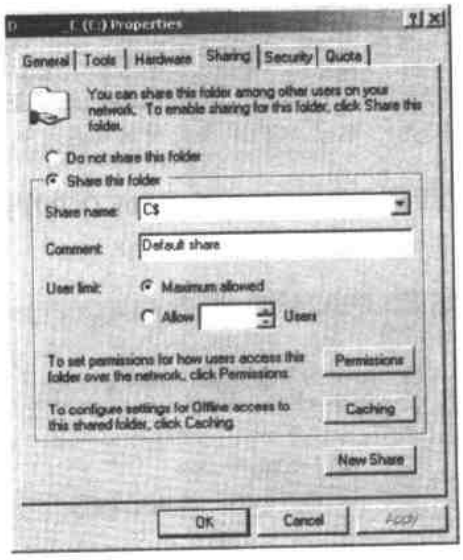

图 5-12　使用 Sharing 对话框改变文件夹或驱动器的共享特征

为了使用计算机的其他用户访问文件夹或驱动器的内容，可选择 Share This Folder 选项。为了使网络上的其他用户能编辑或删除文件，可以选择 Allow Network Users to Change My Files 选项。

如果允许共享，这个文件夹或驱动器的图标会改变。一个手型图标会将这个共享元素提供给网络。

5.3.3 网络接口适配器选项

可以按照下面的步骤改变网络接口适配器选项：

(1) 打开 Control Panel，双击 Network and Dial-up Connections 图标。Network Connecitons 窗口会出现在屏幕上。

(2) 右击无线接口适配器的网络连接文档的图标。从弹出菜单里选择 Properties。

(3) 在 General 选项卡中，选择 Configure 按钮。Adapter Properties 窗口将弹出。

(4) 单击 Advanced 标签，将显示属性列表。

(5) 将列表中的每个属性醒目显示，观察 Value 栏中的当前设置。有些值是文本字段，有些则是下拉式菜单。如要改变文本栏中的当前值，可以选中当前文本并输入新值。如要改变菜单里的值，可以打开下拉式菜单，选择您想使用的新值。

(6) 单击 OK 按钮保存您的改变并关闭窗口。单击 Network 窗口里的 OK 按钮回到桌面。

有些无线网络适配器，包括一些 Orinoco 产品，不接受任何选项设置。如果没有在 Adapter Properties 窗口里看到 Advanced 选项卡，使用由适配器提供的配置实用程序来改变适配器的设置。

5.3.4　网络标识

在 Windows 2000 里，这个属性设置位于 System Properties 窗口的 Network Identification 选项卡上。按照下面的步骤改变这些设置：

(1) 打开 Control Panel，双击 System 图标。System 窗口会出现在屏幕上。

(2) 单击 Network Identificaiton 标签，会出现如图 5-13 所示的对话框。

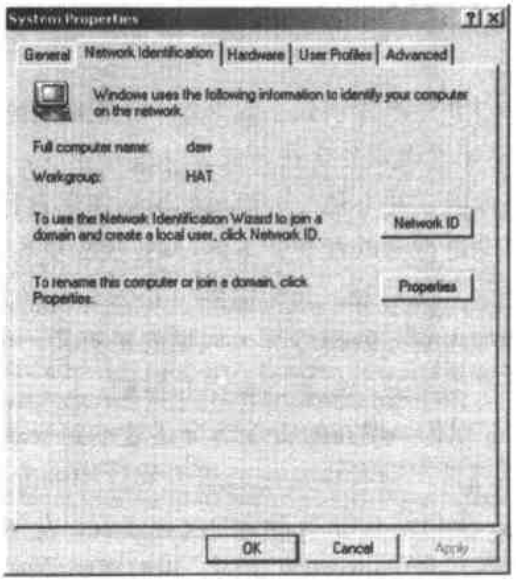

图 5-13　Network Identification 对话框显示计算机的当前标识

(3) 单击 Properties 按钮可以打开 Identification Changes 窗口，如图 5-14 所示。

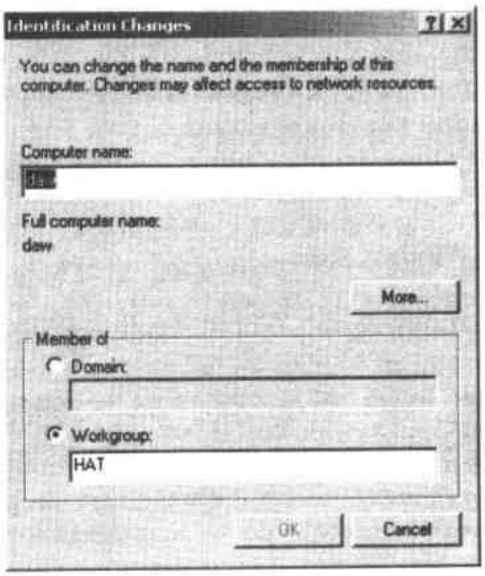

图 5-14　用 Identification Changes 窗口设置计算机名和网络的 SSID

(4) 在 Computer Name 栏里输入在网络上标识您的计算机的名称。

(5) 在 Workgroup 栏里输入网络的 SSID 值。

(6) 单击 OK 按钮保存设置，然后关闭窗口。

5.4　配置 Windows XP

Microsoft 在 Windows XP 系统中引入了对 802.11b 无线网络的特定支持，它将无线网络配置和其他 Windows 配置设置整合在一起。从理论上讲，这应该可以使我们更方便地建立和使用无线网络，但它并不是一个简单的即插即用过程。

这样做的目标就是自动进行无线配置；Windows 应提供自动检测无线网络适配器和搜索可访问的无线网络信号的功能。当检测到一个邻近网络时，Windows 应允许用户只需单击几次鼠标就能加入到无线网络里。如果您想更换一个不同品牌的适配器(假设可被 XP 支持)，您就不必学习另一组新的命令和控制。

这只是目标，由于很多原因，现在的实际情况还达不到要求。首先，自动配置特性需要无线适配器中的兼容固件，但很多适配器里没有这样的固件。其次，与无线配置工具相比，Device Manager 里仍然有很多难懂的配置设置。在 Windows XP 的支持得到改进，以及更多的适配器兼容 Windows XP 之前，我们都必须使用由网络适配器自带的配置工具和不是很清晰的网络配置设置和选项。

5.4.1　您是否有最新的固件

由于许多网络适配器制造厂商已经花费很多时间来制造与 Windows XP 兼容的固件，因此确保使用最新的软件和适配器固件就显得更为重要。几乎每个适配器厂家都会在它们的免费下载 Web 站点中提供最近的更新产品。

5.4.2　使用 Windows 无线工具

如果您的无线适配器支持 Microsoft 的配置工具，您就应该试试它。有些厂家已经将它们自己的程序与 Windows Wireless Properties 控制程序整合在一起，而有些则完全将这个过程交给 Windows 实用程序。例如，图 5-15 是 Orinoco Client Manager。当您从 Actions 菜单里选择 Add/Edit Configuration Profile 选项时，Windows 的 Wireless Networks Properties 窗口就会弹出。

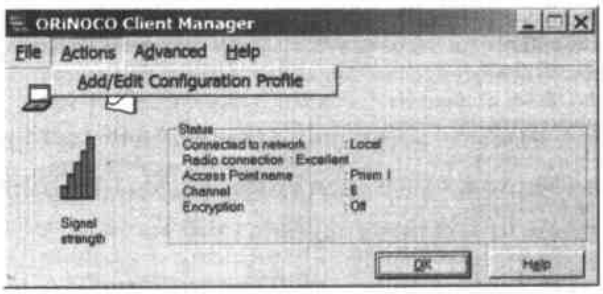

图 5-15　选择 Orinoco 的 Client Manager 的 Add/Edit Configuration Profile 选项后，将打开 Windows Wireless Networks Properties 配置工具

其他适配器允许您在它们自己的程序和 Windows 工具之间选择。这两个程序都能完成同样的工作，这样正确的选择就是使用您自己最喜欢的。两个都试用一下，使用简单而又易用的一个。

5.4.3　无线网络连接状态

要打开状态窗口，请双击系统面板中靠近时钟显示的网络图标。

Wireless Network Connection Status 窗口显示了当前无线连接的状态，包括连接的状态、当前连接的总活动时间、数据传输速率、信号质量以及适配器从连接到网络开始所发送和接收到的字节数。图 5-16 显示了一个状态窗口。

要关闭无线电连接，单击 Disable 按钮(位于状态窗口的最低端)。要改变大部分常

规的网络设置，单击 Properties 按钮。

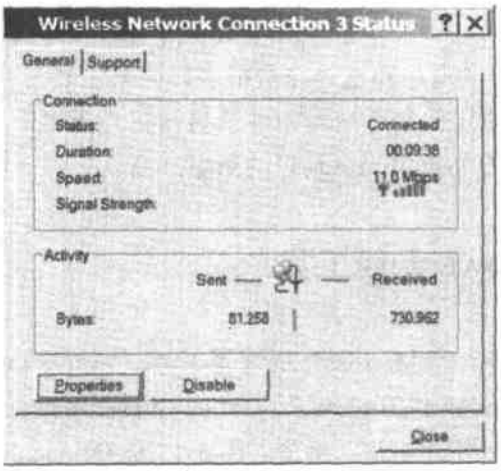

图 5-16　Windows XP 中的 Wireless Network Connection Status 窗口

5.4.4　网络配置设置

要改变无线网络配置选项，可选择 Start | Settings | Network Connections，然后双击无线连接图标。Wireless Network Connection Properties 窗口与有线网络连接的属性窗口类似，只是多了一个无线选项的选项卡，如图 5-17 所示。

图 5-17　选择 TCP/IP 条目设置网络选项

可以按照下面的步骤进行无线连接的配置：

(1) 在已安装条目的列表里选择 Internet Protocol(TCP/IP)条目，然后单击 Properties 按钮。将弹出一个 TCP/IP 属性窗口，如图 5-18 所示。如果没有选择 General 标签，请选择它。

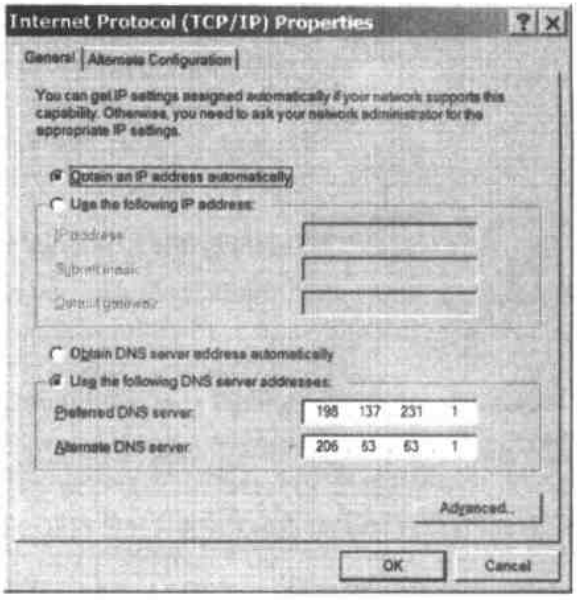

图 5-18　控制网络连接选项的 TCP/IP Properties 窗口

(2) 如果网络里的接入点或其他设备的 DHCP 服务器已经开启，选择 Obtain an IP Address Automatically 选项。如果没有使用 DHCP 服务器，就选择 Use the Following IP Address 选项，然后在 IP Address 栏中输入分配给这台计算机的 IP 地址。

(3) Subnet Mask 栏可以在控制 IP 地址的 TCP/IP Properties 窗口中找到。如果您的网络里没有使用 DHCP 服务器，输入接入点所用的子网掩码。

(4) 如果没有使用 DHCP 服务器，在 Default Gateway 栏中输入无线接入点的局域网 IP 地址。

(5) 如果 DHCP 服务器为网络客户机分配了 DNS 地址，选择 Obtain DNS Server Address Automatically 选项。如果网络使用了静态 DNS 服务器，选择 Use the Following DNS Server Address 选项，然后输入您的网管或 Internet 服务供应商提供的 DNS 地址。

(6) 单击 OK 按钮保存设置，然后关闭窗口。

5.4.5　文件和打印机共享

为了使其他网络用户可以使用文件夹或整个驱动器的内容，右击文件夹或驱动器的图标，然后从下拉菜单里选择 Sharing and Security 选项。打开的 Properties 窗口如图 5-19

所示。

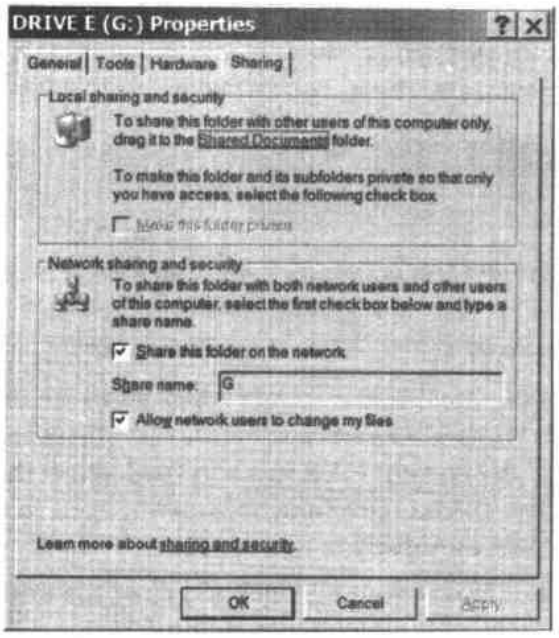

图 5-19　用 Properties 窗口的 Sharing 选项卡设置文件夹或驱动器的共享特征

为了限制对文件夹或驱动器的网络访问，可以选择 Share this Folder on the network 选项。如果允许网络上的其他用户编辑或删除文件，可以选择 Allow network users to change my files 选项。

如果您已经设定了一个文件夹或驱动器为共享，那么它们的图标将会改变。一个手型图标会将这个共享元素提供给网络。

5.4.6　网络接口适配器选项

可以按照下面的步骤改变网络接口适配器选项：

(1) 从 Wireless Network Connection Properties 窗口里单击 Configure 按钮。Adapter Properties 窗口将出现在屏幕上。

(2) 单击 Advanced 标签，将显示如图 5-20 所示的属性列表。

(3) 将列表中的每个属性醒目显示，观察 Value 栏中的当前设置。有些值是文本字段，有些则是下拉式菜单。如要改变文本栏中的当前值，可以选中当前文本并输入新值。如要改变菜单里的值，可以打开下拉式菜单，选择您想使用的新值。

(4) 单击 OK 按钮保存您的改变，并且关闭窗口。单击 Network 窗口里的 OK 按钮回到桌面。

图 5-20　使用适配器的 Properties 窗口中的 Advanced 选项卡配置网络适配器

有些无线网络适配器并不接受任何可选设置。如果您没有在适配器的 Properties 窗口中看到 Advanced 选项卡，那么可以使用由适配器提供的配置实用程序改变适配器的设置。

5.4.7　网络标识

如果要在 Windows XP 中设置或改变计算机名称，请打开 System Properties 窗口中的 Computer Name 选项卡。按照下面的步骤改变这些设置：

(1) 打开 Control Panel，双击 System 图标。System Properties 窗口将出现在屏幕上。

(2) 单击 Computer Name 标签，将显示如图 5-21 所示的对话框。

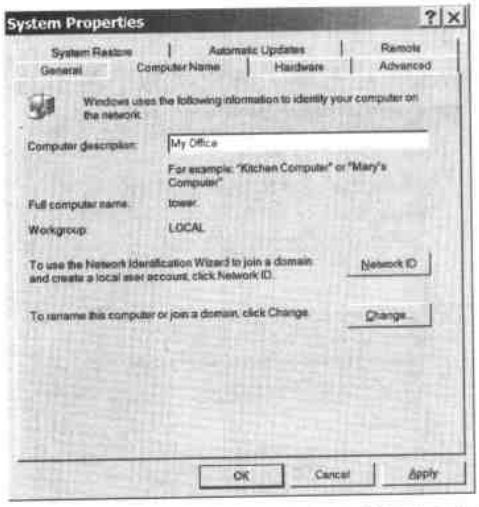

图 5-21　用 Computer Name 选项卡改变计算机名和网络的 SSID

(3) 在 Computer Description 里输入在网络上标识您的计算机的名称。

(4) 单击 Change 按钮。弹出 Computer Name Changes 窗口，如图 5-22 所示。

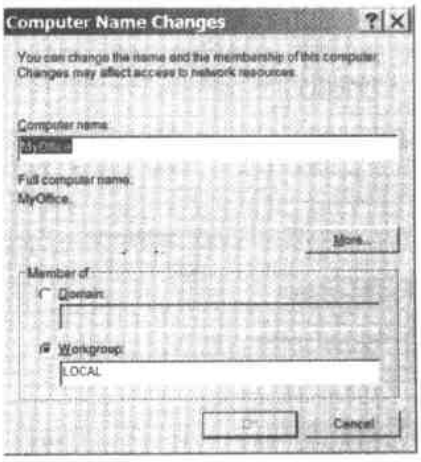

图 5-22　使用 Computer Name 选项卡改变计算机名称和网络的 SSID

(5) 在 Workgroup 栏里输入网络的 SSID。

(6) 单击 OK 按钮保存设置，然后关闭窗口。

5.4.8　在 Windows XP 中配置无线网络

Windows XP 中的无线配置工具被设计成可以控制很多品牌无线适配器的通用接口。有些适配器厂商专门使用 Windows 实用程序，而有的则将它当作自己更广泛的网络配置程序包中的一部分。

可以按照下面的步骤打开 Wireless Network Connection Properties 窗口：

(1) 双击 Windows 系统面板中屏幕右下角靠近时钟的 Network 图标。将弹出 Wireless Connection Status 窗口。

(2) 单击窗口底部的 Properties 按钮。弹出类似于图 5-23 所示的 Properties 窗口。

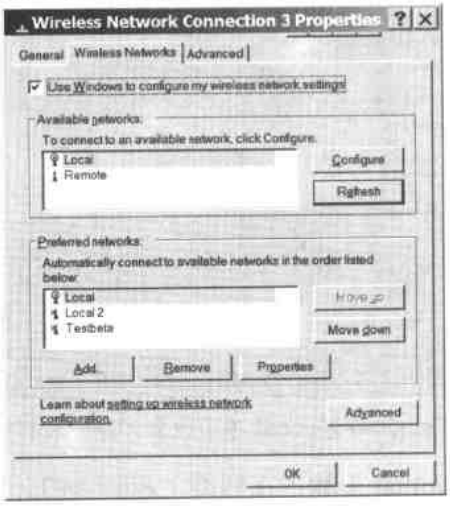

图 5-23　Wireless Network Connection Properties 窗口

1. 选择网络

如果您的计算机处于很多网络覆盖区域中，您必须选择想要使用的一个。Wireless Properties 实用程序包括了一些首选网络的列表，但它并没有限制您必须使用这些列表中的网络。

Properties 窗口中的可用网络列表显示了所有将接受您的无线适配器连接的网络 SSID 值。如果适配器仅检测到一个网络，Windows 会自动连接到该网络上。如果网络适配器检测到很多网络，它会将每个网络的 SSID 与 Preferred Networks 列表中的名称进行比较，然后自动选择有最高优先级的网络。您还能使用 Properties 窗口里的 Move Up and Move Down 按钮对 Windows 搜索网络的顺序重新进行排列。

Microsoft 已经费尽心机地将指定 Windows 是否将限制其仅使用首选网络列表上网络的对话框隐藏了起来。如果您的适配器检测到一个不在首选列表中的网络，而 Advanced 窗口中的非首选选项被激活，系统会建立一个连接。单击 Properties 窗口中的 Advanced 按钮就可弹出该窗口。

当然，计算机选错也是有可能的——如果它检测到两个以上的网络，它就不会自动连接到您想要连接的网络。当这种情况发生时，在 Available Networks 列表里选择正确网络的 SSID，然后单击 Configure 按钮。这样会打开另一个关于该网络更多信息的窗口，这样就会建立与这个网络的连接。

2. 将加密开启或关闭

可通过主 Properties 窗口的 Configure 按钮或 Properties 按钮打开 Local Properties 窗口，它包含了一些 WEP 加密选项。如果正在使用 WEP 加密被激活的网络，请选中 Data Encryption 选项。

5.5　小结：建立连接

无论您使用的是 Windows XP 还是其他早期的操作系统，都可以建立起一个无线网络连接。如果不能运行自动连接功能，不要认为您做错了什么——更可能的是，您只是一个设计得较差产品的受害者。下面提供了几种检查方法：

- 您计算机上的 SSID 是否与您想要连接的网络的 SSID 相同？
- WEP 加密模式是开或关？如果开着，查看是否使用了正确的加密密钥？加密被设定为 64 位还是 128 位？
- 接入点是否使用了 MAC 地址过滤？您的无线适配器是否在合格用户列表之中？

- 工作组的名称是否和 SSID 相一致？
- 接入点是否使用了 DHCP 服务器？如果没有，IP 地址、子网掩码和默认网关有没有设置正确？
- 前导长度的设置是否正确？

第6章　Macintosh下的Wi-Fi

Apple 的 AirPort 无线网络产品家族是 Macintosh 用户用于将计算机通过无线网络连接起来，以及需要将他们的 Macs 系统连接到一个现有无线网络的合理选择。由于 Apple公司控制了网络链接的两个终端——接入点和网络客户机，因此建立一个 AirPort 网络要比建立一个通用 802.11b 网络要容易得多。AirPort Base Station(Apple 的接入点名称)可以从现有的 Macintosh 连接里自动装载 Internet 设置，同时将这些设置发送到相同网络上的所有其他计算机中。

苹果公司是 Wi-Fi 联盟的成员之一，AirPort Base Station 和 AirPort Card 都已经通过 Wi-Fi 认证。因此，一个带有 AirPort Card 的 Macintosh 可以像它加入 AirPort 网络一样容易地加入到 802.11b 网络中。一个包含有 Macs、基于 Windows 的 PC、Unix 或 Linux 机器的混合平台无线网络同样可以使用一个或多个 AirPort Base Station 作为接入点。

用在 AirPort Card 和 AirPort Base Station 中的无线电设备是 Orinoco PCMCIA 无线网络适配器的专用版本。AirPort Base Station 由 KarlNet 生产，这是一家销售 Wireless KarlRouter 产品的公司。

Apple 公司在它的无线网络中对某些特性和功能使用了不同的名称，但设计、配置和使用 AirPort 网络的一般性规则和建立一个通用无线网络一样。关于 AirPort 网络和其他 Wi-Fi 网络的惟一不同点是一些专业术语，以及可以将配置数据从网络客户机发送到 AirPort Base Station 上的相关软件。

这一章将解释如何在 Macintosh 计算机上建立和使用一个无线 AirPort 网络，以及如何将一台有 AirPort Card 的 Macintosh 加入到现有 802.11b 网络(没有使用 AirPort Base Station)里，还有就是如何将一个运行 Windows 的计算机加入到 AirPort 网络里。

6.1　AirPort 组件

AirPort 产品家族包括两个组件：无线网络适配器(叫作 AirPort Card)和接入点(叫作 AirPort Base Station)。AirPort Card 是一种 PCMCIA 卡，它随一个适合于 Macintosh 模型(仍不支持 PC 卡)中的安装支架提供。AirPort Base Station 是一个管理无线网络的单机接入点。最新的版本包括一个内置的 PCMCIA 槽，其中还包含一个 AirPort Card(一个相同的 WaveLAN 或 Orinoco 无线适配器卡)、两个 10/100Base-T 以太网端口和一个内置的 56Kb/s 电话线调制解调器。图 6-1 所示是一个 AirPort Base Station。

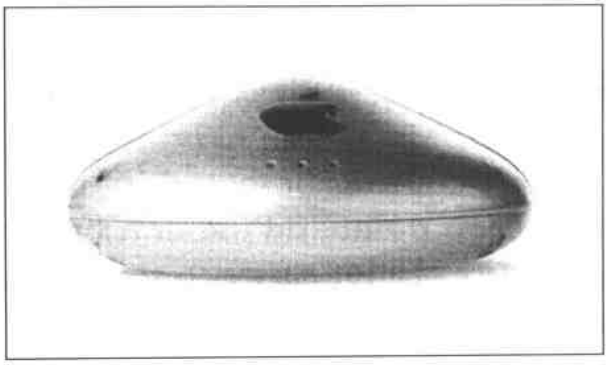

图 6-1　Apple 的 AirPort Base Station，它是经过优化用于 Macintosh 计算机的无线网络设备

AirPort Base Station 通过三个指示灯来显示当前运行状态，如表 6-1 所示。

表 6-1　指示灯显示当前状态

灯	颜　色	状　态
1	闪烁的绿色	正在通信
2	稳定的绿色	通电
3	闪烁的绿色	以太网或调制解调器的端口正在使用

随 AirPort 硬件一起，Apple 还提供了一些软件工具：

- AirPort Setup Assistant，一个自动化大多数网络安装过程的自动配置工具。
- AirPort Admin Utility，可以直接访问设置和改变更复杂的网络的配置选项。
- AirPort Control Strip，从桌面监视和控制网络活动的简单工具。
- AirPort Application，提供更详细地控制和监视网络性能的工具。
- AirPort Software Base Station 程序，使用独立基站的另外一种方法；它可以将一个网络客户机转换成一个由软件控制的接入点。

6.2　建立 AirPort 网络

多数 AirPort 用户可以不用考虑复杂的配置选项，他们只需使用 AirPort Setup Assistant 就可以创建和配置网络。但是，如果实际情况要求您直接控制一些高级选项，或者网管想监视网络的运行，AirPort Admin Utility 可提供对网络设置更完全的控制。

使用 Setup Assistant 可以简单而快速地创建网络：只要配置客户机，单击一些按钮，一切由软件来作决定。Setup Assistant 自动加载所有设置并建立网络。

6.2.1　安装硬件

有些最新的 Macintosh 模型自带内置的 AirPort 适配器和与操作系统捆绑在一起的 AirPort 软件。如果您正在使用一个没有 AirPort Card 的老式 Macintosh 系统，就必须在运行 AirPort Setup Assistant 之前安装 AirPort Card。

可按照下列步骤安装 AirPort Base Station：

(1) 将 AirPort Base Station 安装在您计划操作它的地方。与其他无线网络接入点一样，一个单独的 AirPort Base Station 应该尽量接近您想要覆盖的区域中央。如果您想安装多个基站以覆盖更大区域，将它们在整个空间中均匀分布。

(2) 在基站的以太网端口和当前有线以太网集线器或宽带 Internet 路由器(如 DSL 调制解调器或一个电缆调制解调器)之间拖根电缆线。如果您无权使用有线局域网或宽带 Internet 服务，或者如果您想用电话线路作为宽带连接的备份，那么您可以从基站的调制解调器端口到壁式电话线插座使用标准电话线。

(3) 将电源线插入到基站的电源插座和交流电插座中。

AirPort Base Station 的天线被内置在包装盒中，只能通过移动整个盒子来移动这些天线。在运行完 AirPort Setup Assistant 后，如果发现对所有网络客户机的可靠数据交换来说，信号级别并不是很好，那就有必要将基站移动到另外一个地方来获得更好的信号覆盖度。

6.2.2　运行 AirPort Setup Assistant

AirPort Setup Assistant 的结构在 OS 9 和 OS/X 系统间有些变化，尽管它们可能位于不同的地方，但命令都是相似的。

按照下面的步骤在 OS 9 系统中使用 AirPort Setup Assistant：

(1) 在本地计算机和 Internet 间建立一个直接连接。AirPort Setup Assistant 将把这台计算机的配置设置传输到基站中。

(2) 如果尚未安装 AirPort Card，请安装它。

(3) 确信 AirPort Base Station 已连接到一个电话线路、一个宽带连接或二者，并且电源也已经连接到基站。基站上的 2 号绿灯(中间的绿灯)应该是亮的。

(4) 打开目录的顶级菜单。

(5) 打开 AirPort Setup Assistant，在 Mac OS 9，它位于 Applications/Apple Extras/AirPort；在 Mac OS X 中，位于 Applications/Utilities 目录下。会出现 AirPort Setup Assistant 的 Introduction 屏幕。

(6) 选中 Introduction 屏幕的三个选项中的一个，如图 6-2 所示。

(7) 设置本地计算机与一个现有无线网络的连接。

(8) 设置 AirPort Base Station。

(9) 设置 Software Base Station。

Introduction 屏幕首先提供的是 Set Up Your Computer to Join an Existing Wireless Network 选项，但实际上，在您成功设置本地计算机之前，至少必须有一个基站(或其他接入点)运行在 AirPort Card 的信号范围内。当您在新建一个新网络时，您至少必须先设置一个基站。因此，我们将首先解释 Set Up an AirPort Base Station 选项。

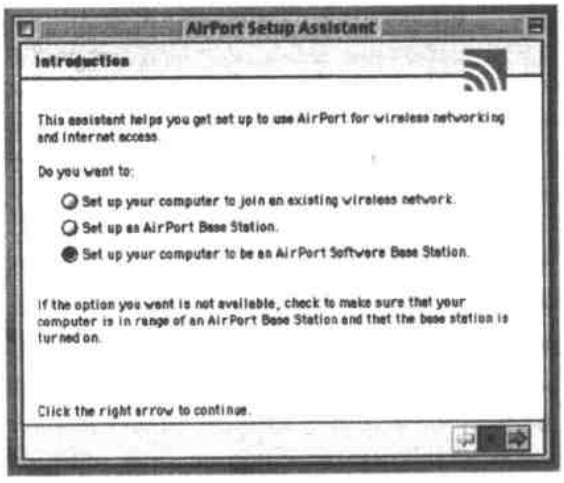

图 6-2　AirPort Setup Assistant 提供了设置本地 AirPort Card、AirPort Base Station 或 Software Base Station 的选择

1. 设置 AirPort Base Station

Internet Choice 选项规定了配置基站的方法。如果正在运行 Setup Assistant 的计算机已经有一个 Internet 连接，程序会使用这些设置来配置基站。如果没有 Internet 连接，Setup Assistant 则会打开 Internet 安装向导，这个向导会请求所有使无线网络连接到 Internet 上的 TCP/IP 配置设置。

2. 在您的计算机和现有无线网络之间建立连接

Set Up Your Computer to Join an Existing Wireless Network 选项会自动检测来自活动网络的无线电信号，并且使本地机器连接一个或多个网络。如果设置完成，计算机会显示一个 Conclusion 屏幕来报告 AirPort Setup Assistant 已经完成，同时还显示一个被检测到的网络的列表。如要加入一个网络，请在列表上选择这个网络名称，然后单击 Connect Now 按钮。

当 AirPort Card 和网络之间建立关联时，计算机会自动运行 AirPort 应用程序。

3. 将计算机设置为 AirPort Software Base Station

Software Base Station 可以通过网络中的一台计算机上执行 AirPort Base Station 的所有功能。使用这个方法时，您可以不用添加一个独立的基站就能提供无线网络，但它会增加运行基站软件的计算机上资源的额外负担(包括处理器功率和内存)，并且这也意味着如果这个基站计算机被关闭，整个网络就不能运行。一个独立的 AirPort Base Station 也允许网管更灵活地安排基站位置。

如果您决定使用 Software Base Station，选择一台尽量在覆盖区域中央的计算机运行基站软件，因为网络上的其他无线客户机需要和基站交换无线电信号。

要安装 Software Base Station，那么可选择 Set UP Your Computer to Be an AirPort Base Station 选项。Setup Assistant 会让您选择自动从您计算机的 Internet 设置中导入网络配置数据，或者是打开 Internet Setup Assistant。

6.2.3　AirPort 应用程序

AirPort 应用程序是由其他无线网络适配器提供的基于 Windows 配置和状态软件的 Apple 版本。图 6-3 所示为 AirPort 应用程序。

图 6-3　AirPort 应用程序显示本地计算机无线网络连接的当前状态

AirPort 应用程序由三个部分组成：Status、AirPort 和 AirPort Network。

1. Status

Status 部分显示了当前与该计算机相关联的网络名称、连接状态和 AirPort Card 正在接收的信号质量。

2. AirPort

AirPort 部分显示了 AirPort Card 当前是开或关，另外还提供一个按钮以开启或关闭卡。AirPort ID 是本地 AirPort Card 的 MAC 地址。

当网络被配置成一个封闭网络时，它不会显示检测到的网络列表。为了连接到一个封闭网络，用户必须在 AirPort Application 或 Control Strip 里键入网络名称。这也是 AirPort 可以防止未授权用户进入网络的一个安全特性。

3. AirPort Network

在 AirPort 网络下的 Choose Network 菜单是由网络客户机所检测到的所有无线网络的列表(除了封闭网络)。

Computer-to-Computer Network 选项将本地网络客户配置成特别网络的成员。

Base Station ID 是 AirPort Base Station 的 MAC 地址，或者是控制当前与这个客户机连接的网络的其他接入点的 MAC 地址。

6.2.4　AirPort Control Strip 模块

AirPort Control Strip 模块(如图 6-4 所示)以五个圆圈显示当前信号的质量；填充的圈越多，信号质量就越好。AirPort 模块也是一个能打开菜单的控制按钮，用户可通过菜单执行一些通用功能。

- 将无线网络连接开启或关闭。
- 如果区域中有多个无线信号时，选择一个网络连接。
- 通过基站的调制解调器建立一个连接。
- 监视和控制调制解调器的活动。
- 显示本地计算机和基站的 AirPort ID(MAC 地址)。

图 6-4　从桌面提供访问基本 AirPort 网络控制的 AirPort Control Strip 模块

6.2.5　AirPort 管理实用程序

您很可能只需使用 Setup Assistant 的默认配置设置就可以设置一个 AirPort 网络，在 Setup Assistant 不能提供足够选项时，AirPort 管理实用程序还提供了一个建立或改变这些设置的方法。

OS 9 中的 AirPort Admin Utility 窗口有 4 个选项卡，每一个都包含对 AirPort 程序

不同部分的控制。在 OS/X 系统里则有 6 个选项卡，但命令和功能与 OS 9 里类似。

1. AirPort 选项卡

Admin Utility 的 AirPort 选项卡包含对 AirPort Base Station 和网络的总体控制。当前连接到网络的所有 Macintosh 计算机都能访问这些控制。图 6-5 显示了 AirPort 选项卡。

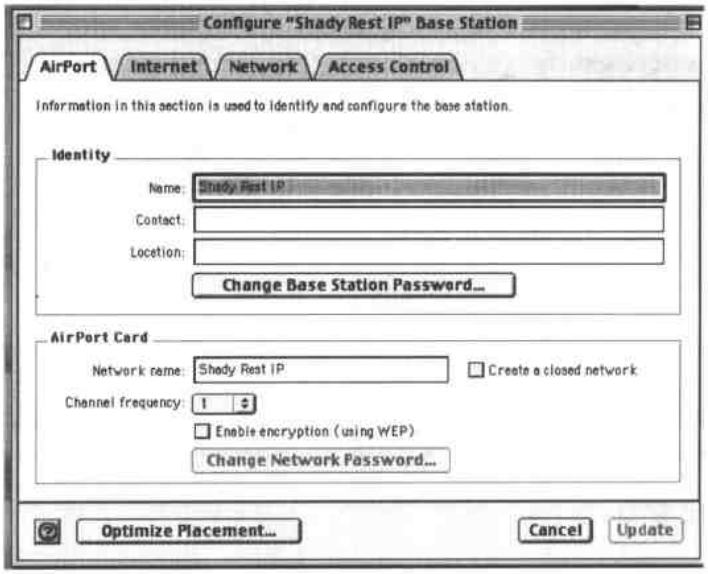

图 6-5　包含网络控制的 AirPort 选项卡

该窗口的 Identity 部分中的信息指定了 AirPort 网络的名称，这与其他 802.11b 网络的 SSID 相同。为了将一台没有 AirPort 无线适配器的计算机连接到一个 AirPort 网络上，您需要使用这个网络名称作为 SSID。

Contact 和 Location 栏是显示该网络其他信息的可选设置。一般来说，Contact 栏可以包含网络维护人的名字、电话号码或是 email 地址，而 Location 栏可以是基站的物理地址。

AirPort Card 部分重复网络名称，并且提供了改变 Channel Frequency(无线电频道的频率)的位置，这是 Apple 为无线电频道号所起的名称。AirPort 网络的默认频道号是 Channel 1，但它仍和其他频道一样。在有多个 AirPort Network 运行的环境中，每个网络必须使用一个不同的频道。所有能防止来自其他 802.11b 网络或 2.4GHz 无线电波服务干扰的规则都适用于 AirPort 网络，因此最好不要使用那些默认的频道号。当基站改变频道时，所有连接到该网络的 AirPort 客户机会自动转换到这个新频道。在一个混合平台网络里，绝大多数 802.11b 网络适配器会搜索活动的网络信号，这样您就可以希望网络客户机自动转换到新的频道上。如果网络上没有适配器能自动转换频道，那么就必须手动设置频道。

Create a Closed Network 选项允许网络管理员创建一个无线网络，这个网络的名称不会出现在 AirPort Setup Assistant、AirPort 应用程序、AirPort Control Strip 模块的可用网络列表中。为了连接到一个封闭网络，用户必须键入网络的名称，而不是从列表中选择。

Optimize Placement 按钮会打开如图 6-6 所示的 Placement 窗口。

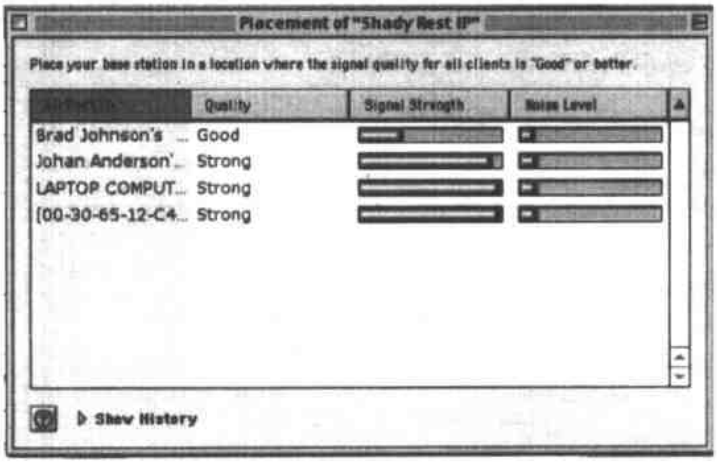

图 6-6　显示来自每个网络客户机的信号质量的 Placement 窗口

2. Placement 窗口

Placement 窗口图形化显示了当前连接在该基站上的每个网络客户机的信号质量和信号强度。这个显示可以帮助网管选择一个基站或客户计算机的最佳位置。

AirPort ID 列显示了每个连接在该无线网络上的计算机名称。如果计算机没有被分配名称，AirPort ID 列则会显示出这台计算机的 MAC 地址。

Quality 列显示基站检测到的无线电连接的信号质量。质量是信号强度和噪声级别综合得到的物理量，因此一个较强但噪声很大的信号的质量则会比处于消声地区的较弱信号的质量要差。如果链接的信号质量是“好”或更好，它就可以在全速条件下交换数据。

Signal Strength 列显示了从每个网络客户机到基站所测到的无线电信号强度。

Noise Level 列显示了基站从每个链接上所接收到的其他网络和无线电服务的干扰量。当噪声级别达到信号级别时，网络性能将降低。

Show History 选项会打开另外一个显示历史网络信号质量的图形化界面。

3. Internet 选项卡

Internet 选项卡(如图 6-7 所示)指定了基站用于将本地无线局域网连接到 Internet 的相关信息。AirPort Setup Assistant 会自动加载这些设置。

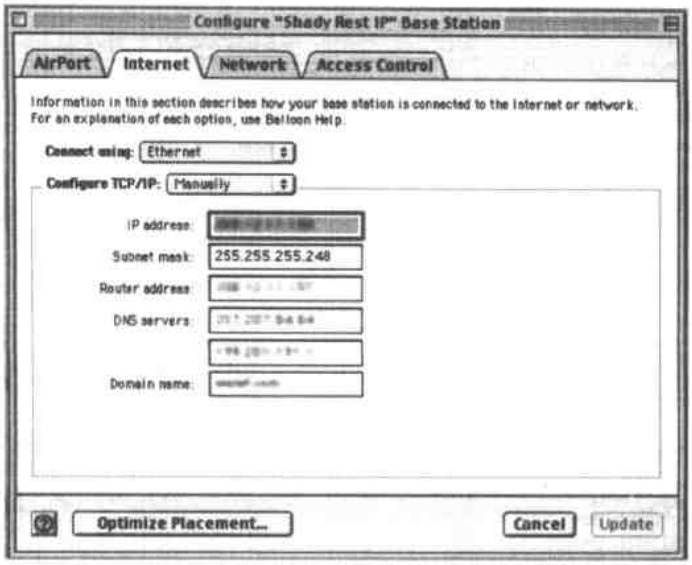

图 6-7　Internet 选项卡包含了 TCP/IP 连接选项并选择 Internet 连接类型

有些设置会随时间改变(例如一个 Internet 服务供应商重新配置它的网络服务器)，因此，AirPort Admin Utility 可提供对网络配置设置的访问：

- Connect Using 选项允许网管通过基站的以太网端口或内置调制解调器指定一个连接。当 Connect Using Modem 激活时，基站可以通过一个呼叫电话将无线网络连接到 Internet 上。当 Connect Using Ethernet 激活时，基站可以通过局域网连接将网络客户机连接到 Internet 上。
- 两个 Configure TCP/IP 选项可用：由 DHCP 选项通知基站为每个客户机分配 IP 地址和子网掩码；而 Manual 选项则需要用户在每台计算机上手工键入这些设置。
- IP Address 栏显示了这台网络客户机上 Internet 连接的数字 IP 地址。
- Subnet Mask 栏显示了基站用于通过单个 Internet 连接将多个客户机连接在一起的子网掩码设置。
- Router Address 栏是网络的 Internet 网关服务器地址。
- DNS Server 栏包含了 Domain Name System 服务器的地址，它将 Internet 域名转换成数字地址。
- Domain Name 栏是将这个客户机连接到 Internet 上的 Internet 域名。

4. Network 选项卡

Network 选项卡(如图 6-8 所示)控制无线 AirPort 网络和有线局域网之间的网桥。

当选中 Distribute IP Addresses 选项时，无线网络上的计算机就可以共享一个数字 IP 地址(网络会将它们内部转换为独立的本地地址)，或者是为每台计算机使用一个独立

的 IP 数字地址。

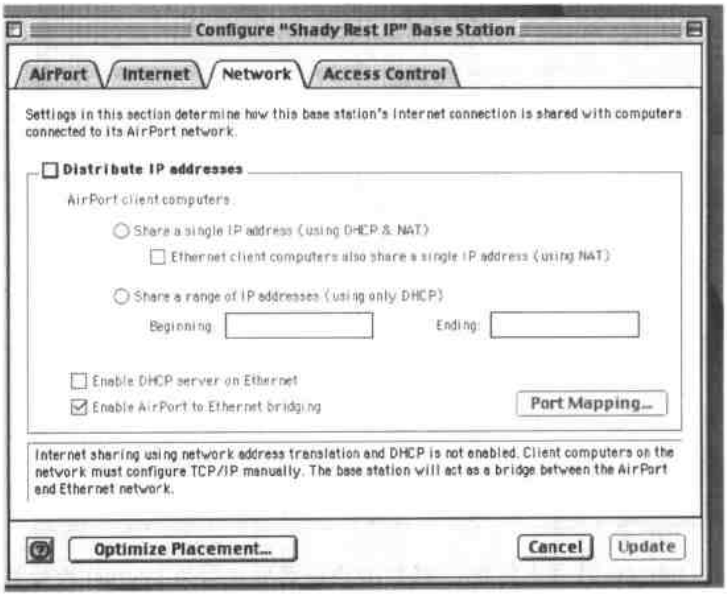

图 6-8　Network 选项卡控制无线 AirPort 网络和有线以太局域网之间的网桥

5. Access Control 选项卡

Access Control 选项卡(如图 6-9 所示)可以将网络的使用权限制在特定计算机上，而不是允许基站接受来自可用信号范围的任何客户机连接。已接受的计算机的列表显示了这些计算机的 AirPort ID。为了将一台非 AirPort 设备加入到一个限制访问的网络里，您可以使用无线网络适配器的 MAC 地址。

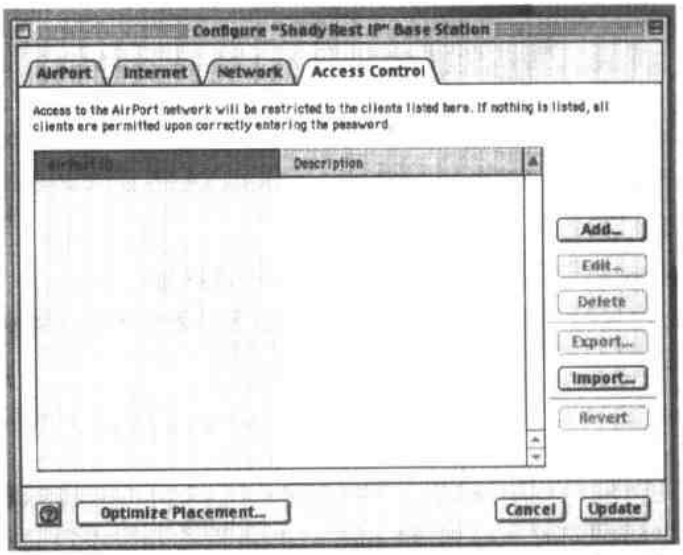

图 6-9　Access Control 选项卡是限制网络访问的安全工具

6.2.6　使用 AirPort 网络

一旦 AirPort 网络建立并运行，Macintosh 会将通过无线链接连接到这个网络上的计算机看成和其他网络资源一样。如果都通过以太网电缆进行连接，文件传输、Internet 访问、远程打印机和其他服务会以相同方式显示在目录上。

对大多数用户来说，无线连接被激活的惟一指示就是在屏幕下面的 AirPort Control Strip 模式的指示灯，当无线电波信号质量由于干扰和网络活动而改变时，这些灯就会时亮时暗。除非网络计算机处于基站覆盖区域的边缘地区，或者它受到了很大的干扰，否则本地网络和 Internet 连接应该快捷而清晰，如同通过 10Base-T 网络一样。

6.3　将 Macintosh 客户机连接到其他网络上

Apple 希望大部分 Macintosh 用户使用他们的 AirPort Card 将计算机通过 AirPort Base Station 连接到其他 Macs 上。但无线网络的使用并不局限在 Macintosh 上。由于 Setup Assistant 将安装过程自动化，将 Macs 连接到一个 AirPort 网络要比构建一个使用其他接入点、网络适配器和配置软件的混合型网络要容易得多，但 AirPort Card 也满足 Wi-Fi 规范的互操作性，因此它们也应该能和其他厂家的 802.11b 接入点进行通信(在特别网络中)。因此，在一个也包括运行 Windows 或其他操作系统的网络客户机的新的或已有无线网络中，使用 Macintosh 计算机应该不是问题。

例如，将计算机带到无线网络服务的办公室和其他公共场所的 PowerBook 用户，他们可以像使用基于 Windows 的笔记本电脑用户一样方便地连接到这些网络上。同时，一个办公室或家庭的无线网络应该可以同时为 Macs 和 PCs 提供服务，而不需改变任何网络配置。

多数 Macintosh 用户希望使用 AirPort Card，而不是其他品牌的无线适配器，因为 AirPort 软件与 Mac OS 的网络功能整合得很好；但也可能安装其他品牌的 PC Card 或基于 USB 的无线网络适配器，当然您必须找到计算机所用的 Mac 操作系统版本上的驱动程序和控制软件。另外，Macintosh 驱动程序还可以用在 Orinoco、Proxim 和 Buffalo 所售的适配器上。Orinoco 适配器和 AirPort Card 的设计很相似(不用感到奇怪，因为它们出自同一个厂家)，同时有些用户已经声称能够使用 Orinoco 的控制软件控制他们的 AirPort Card。

将 AirPort Card 连接到非 AirPort 接入点上

当一台带有 AirPort Card 的 Macintosh 处于一个非 AirPort 接入点提供的信号覆盖区域时，AirPort Card 应该可以检测到网络信号，并且在 AirPort 应用程序的 Choose Network

和 AirPort Control Strip 菜单中显示这个接入点的 SSID 值。如果用户从菜单中选择了这个网络，AirPort Card 就可以和这个接入点建立关联，就像它们和 AirPort Base Station 建立关联一样。Control Strip 模块和 AirPort 应用程序都会图形显示来自该接入点的信号质量，显示方式与连接到 Apple Base Station 一样。

在多数大型商业网络和公用无线服务中，网管可能都为想在无线局域网中使用他们的便携式计算机或其他设备的雇员和访问者提供一份“如何连接我们的网络”文档。这份文档可以是一份打印出来的薄纸片、小册子或在线 Web 页。不管采用什么方式，它都应该包括一些用户必须在他们的配置实用程序里改变的特定设置。AirPort 适配器的配置程序应该是 AirPort Admin Utility，但 Apple 已经为某些设置使用了不同的名称，如“Network Name”(SSID)和“AirPort ID”(网络适配器的 MAC 地址)。幸运的是，AirPort 程序会自动检测网络名称和 ID，这样您就不用手工设置它们。

如果这个无线网络在接入点或网络的其他地方使用 DHCP 来为网络客户机分配 IP 地址，打开 AirPort Admin Utility 的 Internet 选项卡，将 Configure TCP/IP 选项设置为接受 DHCP 地址。

如果网络没有使用 DHCP，网管将提供一张分配给该客户机的配置设置的列表。为将 AirPort 客户机配置到网络上，设置 Configure TCP/IP 选项为 Manually，并且在 AirPort Admin Utility 的 Internet 选项卡里键入这些地址。将网管提供的 IP 地址、子网掩码、DNS 服务器和域名直接复制到 Admin Utility 的相应栏里。AirPort 称为“Router Address”的设置对网络里其他部分来说就是网关。在 AirPort Admin Utility 的 Router Address 栏里填入网管所提供的网关地址。

6.4 将其他 Wi-Fi 客户机连接到 AirPort 网络上

如果无线局域网使用 AirPort Base Station 作为它的接入点，那么该网络并非只限于 AirPort 客户机。AirPort 网络上的各个客户计算机不一定都是 Macintosh。在 AirPort 网络和其他 802.11b 网络之间绝对没有区别，因此一台使用其他品牌的网络适配器和不同操作系统的计算机同样可以检测到 AirPort 网络。

使用其他操作系统的计算机中的网络适配器会将 AirPort Base Station 当作标准的 802.11b 接入点。适配器会使用 AirPort 网络和其他计算机进行数据交换，同时还可以作为 Internet 的网关。在适配器看来，连接到 AirPort Base Station 和连接到其他品牌的接入点没什么区别。

检测无线电信号比较容易，但要配置一个使用网络的网络客户机则要更为复杂，这是因为 Apple 为那些标准的网络配置设置使用了不同的名称。如果不知道如何转换 AirPort 的术语和 802.11b 的术语，您就可能在使网络正常工作时遇到麻烦。不过不必担心，我们会提供帮助。它并不像看起来那么复杂，您只需掌握下面要介绍的内容就可以了。

6.4.1　网络属性

在 Windows 中，Network Properties 窗口包括计算机必须用于连接到一个 TCP/IP 网络的设置和选项。而在 Macintosh 里，同样的信息则是出现在 AirPort Admin Utility 中。

如果 AirPort Admin Utility 被设置为使用 DHCP 配置 TCP/IP，客户机的配置实用程序也必须被设置为接受 DHCP(在 Windows 中，选择 Obtain an IP Address Automatically 和 Obtain DNS Server 选项)。

如果 AirPort 被设置为手动配置 TCP/IP，Windows、Unix 或 Linux 用户必须输入下面的 TCP/IP 属性设置：

IP 地址	使用局域网管理员或 ISP 提供的 IP 地址。
子网掩码	从 AirPort Admin Utility 的 Internet 选项卡内复制地址。如果您不知道地址，可尝试 255.255.255.0。
DNS 服务器	从 AirPort Admin Utility 的 Internet 选项卡复制 DNS 服务器地址。
主机	从 AirPort Admin Utility 的 AirPort 选项卡复制网络名字。
Domain(域)	从 AirPort Admin Utility 的 Internet 选项卡复制域名。
网关	从 AirPort Admin Utility 的 Internet 选项卡复制路由器地址。

6.4.2　无线网络配置

每个无线网络适配器都会自带一个不同的配置实用程序。在 Windows XP 中有一个标准的无线配置实用程序，但如果您正使用一个 Windows 早期版本(或其他操作系统)，将必须使用适配器硬件所提供的程序。

有些配置实用程序自动搜索附近的无线网络，并且显示一个列出每个网络的 SSID 的菜单，而其他程序则需要用户设定需要使用的网络的 SSID 值。如果网络适配器检测到一个 AirPort 网络，它同样会显示 Network Name 的值，并将它作为 SSID。如果配置实用程序请求一个 SSID，使用在 Admin Utility 的 AirPort 选项卡里出现的 Network Name。

如果适配器不能自动选择操作频道，将频道号设定为 AirPort 中设置的 Channel Frequency。

如果网络使用了一个 AirPort Base Station，它就是一个基础网络。如果要在 Macintosh 和 Windows(或其他系统)客户机之间建立一个特别网络，在 AirPort Setup Assistant 的 Settings 屏幕中将 AirPort Network 选项设置为使用 Computer-to-Computer 网络。

一旦网络配置完成，并且客户机和基站建立关联，网络客户机上显示的信号质量就应该显示该链接的质量，而且 AirPort Placement 窗口将显示网络客户机的名称和无线电

链接的质量，以及无线网络上的所有其他计算机。这样，这个网络上的所有计算机(不管是什么操作系统)都将出现在其他计算机的可用网络连接列表中。

6.5 从非 AirPort 客户机配置 AirPort Base Station

一个包含 Macintosh 和其他操作系统的混合网络的管理员可以有两个选项来建立基站：使用一个 Macintosh 配置基站，或者使用 Apple 和其他软件开发商开发的 Windows 和 Unix 的 AirPort 配置程序。

至少有三家软件开发商提供 Apple 自己的 AirPort Base Station 配置软件的代用品。这些软件多数可以用于 Windows 或其他系统，但至少有一个也可用于 Macintosh 系统。

这些程序有着和 Apple 软件一样的功能，但它们组织配置选项的方式不一样。这些程序使用标准 802.11b 和 TCP/IP 术语，这样它们在多数有经验的无线网管看来都不会产生什么迷惑。

6.5.1 Windows 的 AirPort Admin Utility

Apple 公司用于 Windows 的 AirPort Admin Utility 可以从 http://docs.info.apple.com/article.html?artnum=120093 上免费下载。这个程序不能用在早先的 Graphite AirPort Base Station 上，但可以用在新的 Snow 版本上。

顾名思义，Windows 的 AirPort Admin Utility 和 Macintosh 的 AirPort Admin Utility 执行同样的功能。

6.5.2 AirPort Base Station Configurator

Jon Sevy 的 AirPort Base Station Configuratior 是一个 Java 程序，可以运行在任何有 Java Runtime Environment(Java 运行时环境)的主机上，该环境包括 Windows、Unix 和 MacOS 等操作系统的大多数版本。程序(包括一个完整的手册)可从 http://edge.mcs.drexel.edu/GICL/people/sevy airport 上下载。图 6-10 显示了这个程序的一般屏幕。

其他一些 AirPort 实用程序都可用同样的方式获得，包括监控基站上调制解调器活动的程序，测量无线链接信号强度和质量的程序，以及显示当前所有连接到基站的客户计算机列表的 Wireless Host Monitor。

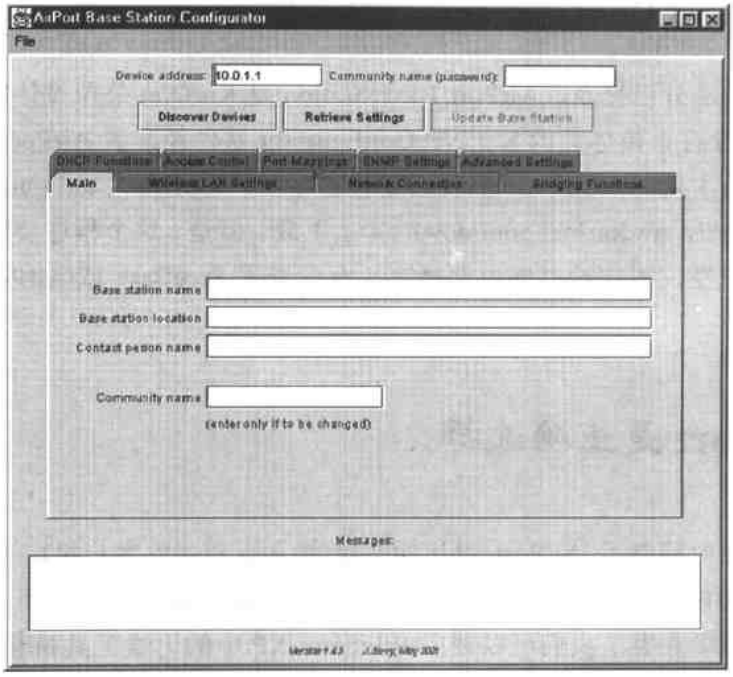

图 6-10　AirPort Base Station Configurator 以人们更喜欢的方式组合所有的配置选项

6.5.3　FreeBase

FreeBase 是一个用于 Windows 的 AirPort Base Station 配置程序，它同样可以在 http://freebase.sourceforge.net 上找到。FreeBase 站点也提供了一个 AirPort Base Station 的“指导性漫游”，其中说明了如何更换内置适配器卡，另外还提供了基站内部通信协议和配置块的详细内容。

图 6-11 显示一个 FreeBase 屏幕。与 AirPort Base Station Configurator 一样，FreeBase 将所有元素都放在一个单选项卡窗口中。

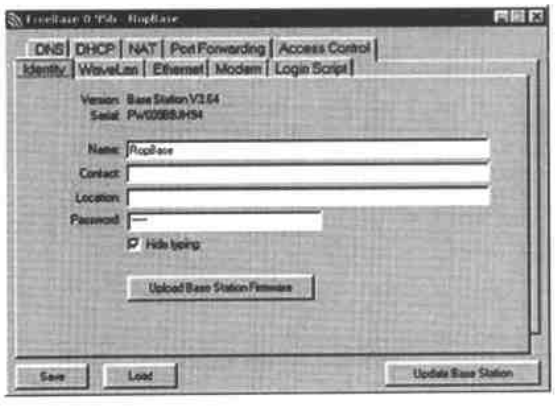

图 6-11　FreeBase 是另一个基于 Windows 的 AirPort Base Station 配置程序

6.5.4 KarlNet Configurator

本章的前面部分已提及，AirPort Base Station 是 KarlNet 公司设计的一种接入点版本。KarlNet 并没有承诺他们的 KarlNet Configurator 软件能配置 AirPort Base Station(可能是不想与它的主要客户竞争)，但我们期望它可以。KarlNet Configurator 的 Windows 版本可以在 http://www.karlnet.com/dowload 上下载。但是，这个程序要比上面的两个程序有更大的局限性，因此没有理由选择它，而应选用 FreeBase 或 AirPort Base Station Configurator。

6.6 AirPort 是正确选择

由于苹果公司控制了 AirPort 设计的两端(接入点和网络客户机)，它提出的系统使配置自动化，而配置对其他大部分无线网络来说，却是棘手问题，而且该系统使用仍与其他 Wi-Fi 网络兼容。我们可以期望 Windows XP 中的无线工具朝着这个方向发展，但就现在来说，将大量 Macs 连接到 AirPort 网络要比连接到其他品牌的接入点上要快捷和简单得多。而且一旦您了解机密的握手协议(以 AirPort 中一些标准特性和功能的古怪名称的形式)，您的非 AirPort 适配器同样也可以很好地在 AirPort 网络中工作。

AirPort 网络实际上是一个多数计算机都使用 Macintosh 的商业或家庭无线网络的首选。在其他情况下，AirPort Base Station(如果必须的话，可以使用第三方软件)也可以是和其他产品媲美的接入点。无论您在关于操作系统的争论里青睐哪一方，AirPort 都是正确选择。

第7章　Linux下的Wi-Fi

任何一种无线网络适配器(除了Apple公司的AirPort卡)都带有Microsoft Windows平台下的驱动程序和配置工具，但这并不意味着Windows是惟一可以让这些适配器工作的操作系统。TCP/IP网络并不关心连接到网络中的计算机正在使用哪种操作系统，它仅仅从一台计算机的端口接收比特和字节并传输出去。因此只要您能够为网络适配器找到合适的驱动程序，那么任何计算机都可以使用无线网络。Windows、Macintosh、Linux以及各种版本的Unix都可以使用无线网络。本章包含了将基于Linux的计算机连接到Wi-Fi网络所需的信息，并且介绍了一些实用程序，以及可以简化以上工作的其他工具。在第8章中，您将找到在Wi-Fi网络上使用带有Unix系统的计算机的类似信息。

要想找到合适的驱动程序并不像听起来那么简单。本章将介绍如何为各种适配器找到合适的Linux下的驱动程序，并且介绍如何安装和使用它们来连接到一个无线网络。如果您从来没有使用过Unix或Linux，那么接入一个无线网络将会非常困难。这一章主要是写给那些已经有足够的Linux经验的用户，来帮助他们设置和使用一个无线网络连接。如果您需要更多的帮助来使用您的Linux客户端，可以求助于您的网络管理员，或者找一本更通俗的Linux入门书作为参考。

7.1　驱动程序及相关内容

在深入学习将Linux设备连接到无线网络前，让我们花些时间来回顾驱动程序如何工作，以及这些驱动程序之所以重要的原因。在本章的后半部分，您将了解如何为不同种类的无线网络适配器找到正确的驱动程序，以及如何使用它们将Linux计算机连接到一个无线网络。

设备驱动程序是介于计算机操作系统和连接到计算机的外围设备输入/输出之间的软件接口。驱动程序包含了一些指令，这些指令用于将从外围设备输入的命令和数据转换成操作系统可以理解的形式，并且将操作系统输出的指令转换成设备特定的控制指令。它进行内存管理和时钟管理，并且指定了输入/输出(I/O)端口和中断号，从而使设备能够和操作系统进行通信。图7-1中显示了计算机和通用设备驱动程序之间的关系。

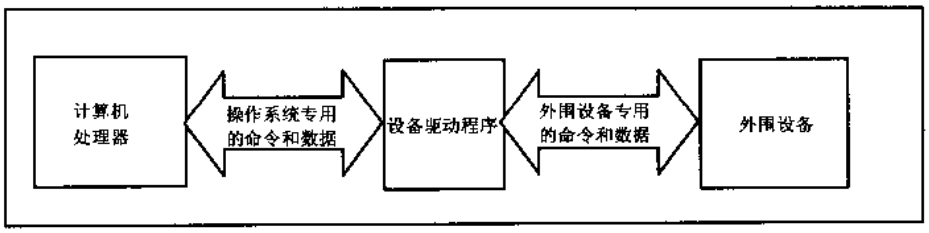

图 7-1　设备驱动程序是计算机与外围设备之间的数据和控制接口

每种外围设备，包括无线网络适配器，都需要一个驱动程序将从计算机获得的标准指令转换成可以处理设备特定功能和特性的控制指令。如果没有驱动程序，设备将无法工作。缺少正确驱动程序的设备就像纸镇或者门挡一样没用。

例如，键盘的驱动程序告诉计算机应该通过哪一个 I/O 端口从键盘中读取数据，或者是将数据发送到键盘，它将按键转换成输入数据，并且控制 CAPS LOCK、NUM LOCK 以及 SCROLL LOCK 灯的开关。打印机的驱动程序包含特定的控制指令，计算机依靠这些指令来区分针打打印机和激光打印机。输入输出设备的驱动程序将指定设备是使用串口、并口、USB 端口和 PCMCIA 插槽，还是使用计算机主板上的一个内部扩展槽。无线网络适配器的驱动程序也将指定一些特性，例如无线电用于发送和接收数据的通道号、无线电的传输功率以及适配器传送数据时的速率等。

无线以太网适配器的驱动程序处理 TCP/IP 通信的物理层——即适配器建立和使用无线电链接到网络所需的信息，而其他的层则处理数据格式和内容。这样就确保了适配器可以处理多种数据格式，而且数据也可以通过多种不同的适配器进行传输。

驱动程序也使相同种类的硬件在不同操作系统中工作成为可能。驱动程序将操作系统产生的输入输出信号与设备的“本机语言”中的命令来回进行转换。为控制同一设备的不同操作系统编写的驱动程序启动时使用不同格式的指令，并且将这些指令转换成一组相同的设备控制。所以，如果您的计算机使用的操作系统是 Linux，那么就需要使用特别为该操作系统编写的设备驱动程序。

将设备驱动程序看作设备的安装手册是非常有用的。该手册分别使用英语、丹麦语、马来西亚语编写，但都包含有一组相同的说明，这样使用不同语言的用户就都可以理解该手册。计算机设备驱动程序也是一样，除了使用的是操作系统的语言，而不是人类的语言。

设备驱动程序是和配置实用程序相分离的软件，但许多软件设计人员将这二者结合成一个安装程序。配置实用程序提供了一组发送指令的命令，并显示驱动程序和网络适配器之间双向的接收数据。

驱动程序的位置

根据以上所述，您必须在使用无线网络适配器前找到适合于计算机所用的操作系统

的驱动程序。如果您运气好，或者在购买时足够仔细的话，随适配器提供的光盘上就可能有正确的驱动程序，或者驱动程序已与操作系统进行了捆绑。

市面上大部分的无线适配器是贴有私人标签的产品，在产品的外包装或者设备上根本没有制造者的名字。因此在使用一个特定的适配器前，您不得不做一些检测工作，从而确定正确的驱动程序。Orinoco 和 Cisco 在私人标签适配器市场上最为常见。适配器的制造商可能不想告诉用户他们的产品包装盒中硬件的制造者，但开发第三方 Linux 驱动程序的人经常会指出各种品牌的产品应该使用的驱动程序。

寻找无线适配器的 Linux 驱动程序的第一个地方是随无线适配器赠送的 CD。一些制造商在提供 Windows 驱动程序时也一并提供了 Linux 驱动程序，但是您不能指望制作商总是提供 Linux 驱动程序。如果已经找到一个驱动程序，虽然您不需要浪费时间去别处再寻找一个，但是可以通过在线升级找到一个更新版本的驱动程序。

如果可以选择，最好在购买适配器时就能得到操作系统所需的驱动程序。生产 Linux 驱动程序的适配器制造商通常做的不错，他们可以使潜在用户很容易得到想要的驱动程序。但在不断发展的无线网络市场上，非 Windows 平台下的适配器驱动程序很难找到。制造商提供的驱动程序也只是被这些制造商做了大概的测试，并且当您向他们求助时，他们的硬件和软件开发人员不会作出指点。世界上没有什么比下面的事更让人生气：某个呼叫服务中心的技术支持人员用单调的声音拒绝回答任何问题，他们的原因仅是“我们不对那个软件提供技术支持”。

随着 Wi-Fi 网络越来越流行，这将更加激励适配器制造商为相对份额较小的市场提供驱动程序。当无线网络用户的总数达到上千万时，那些占份额 5%左右并愿意在 Linux 系统下使用无线网络的用户将成为数目可观的潜在购买者。

如果制造商没有随适配器提供驱动程序，那么您可以到制造商的 Web 站点上去查看是否有免费的驱动程序下载。许多制造商将他们的网址印在适配器的标签上或手册中，但如果找不到网址，那就试试 http://www.[商标名称].com，或者到一个在线的设备驱动目录中查找，例如 http://www.windrivers.com、http://www.driverzone.com 或者 http://www.driversplanet.com。目录站点通常搜集 Windows 下的驱动程序，但如果您沿着一个制造商的驱动程序页面的链接一直找下去，您一般会发现该制造商提供的在其他操作系统下的驱动程序(如果它们存在的话)。

如果您有一块不支持 Linux 的厂家生产的适配器，那么您就得从相对完整和稳定的商业软件世界转向广泛开放的用户组、邮件列表和 Web 站点。那儿有许多用户社团，这些社团由那些渴望改善自己所钟爱的操作系统的性能，以及花费大量时间和雇主资源来共享信息和解答问题的人组成。在这些社团中，大量的软件开发人员为无线适配器开发了设备驱动程序和配置工具。

7.2 Linux 驱动程序

超过 80 种无线网络适配器拥有 Wi-Fi 认证标签，但几乎所有的这些产品都只使用了 4 到 5 种内置芯片组中的一种。因此，要控制每种可能的适配器，只需要几种 Linux 驱动程序即可。

一些公司(包括 Cisco、Intel、Orinoco、Addtron 和 Samsung)通常为他们制造的无线网络适配器提供自己的 Linux 驱动程序。如果不能从适配器制造商那里获得 Linux 驱动程序，那么您可以使用 Linux 发布包中提供的某种驱动程序，或者下载一个第三方开发者提供的独立驱动程序。表 7-1 中包含了部分 Linux 驱动程序的列表。

表 7-1　无线网络适配器的 Linux 驱动程序

适　配　器	驱动程序位置
使用 Intersil Prism II 芯片组的适配器(包括 Actiontec、Addtron、Bromax、Compaq、D-Link、GemTek、Linksys、Nokia、Samsung、SMC、Z-Com、ZoomAir 及其他)	从 http://www.linux-wlan.com/pub/linux-wlan-ng 中下载最新版本的 wlan-ng 驱动程序，或者尝试 http://www.Epitest.fi/Prism2 中的 HostAP 驱动程序。
Orinoco	Linux 驱动程序随适配器的配盘提供，或者到 http://www.orinocowireless.com 去下载。若需要其他的驱动程序信息，可到 http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/ Orinoco.html 中查看。
Apple	AirPort 适配器是使用私人标签的 Orinoco 产品，您可以到 http://www.orinocowireless.com 或 http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Orinoco.html 中下载驱动程序。
BreezeCom DS11	http://www.xs4all.nl/~bvermeul/swallow
Cisco 340 和 350	http://www.cisco.com/public/sw-center/sw-wireless.shtml 这种驱动程序有不同的版本，包含在 Linux PCMCIA 包和 Linux 内核，airo.o 用于 PCI 和 ISA 版本，airo_cs.o 则用于 PCMCIA。
Dell TrueMobile 1100	参考 Cisco 340
D-Link DWL-500	ftp://ftp.dlink.com/Wireless/DWL-500/Driver/DWL500_linux_driver_034.tar.gz
Ericsson 11Mb DSSS WLAN	http://www.ericsson.com/wlan/su_downloads11.asp
Intel PRO/Wireless 2011	http://appsr.cps.intel.com/scripts-df/Product_Filter.asp?ProductID=450

(续表)

适　配　器	驱动程序位置
Lucent	参考 Orinoco(见上)
Nokia C110/C111	http://www.nokia.com/phones/productsupport/wlan/c110_c111/
Samsung Magiclan	http://www.magiclan.com/product/magiclan/download/mlist.jsp
Symbol Spectrum24 High Rate	http://sourceforge.net/projects/spectrum24
3Com AirConnect	http://sourceforge.net/projects/spectrum24
3Com WLAN XJack	http://www.xs4all.nl/~bvermeul/swallow
D-Link DWL-650+及来自于其他供应商的 22Mb/s 产品	在编写这本书时，所有这些适配卡几乎都使用新的 TI 芯片组，而 Linux 并不支持这种芯片组，未来的驱动程序开发可以参考 http://www/hpl.hp.com/personal/Jean_Tourrilhes/Linux

如果在以上的列表中找不到您的适配器，那么可以去查看“Wireless LAN Resources for Linux”网站，它的地址是 http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux。这个站点是关于在 Linux 下使用无线以太网的信息交换中心。并不是这个网站的所有信息都适用于 802.11b 网络，但依然有足够多的有用信息。

Linux 社团以向新用户提供帮助而著称。也许某个人正巧知道您的 Whoopie-Matic Lightning Bolt 无线适配器应该使用何种驱动程序，他会在 Linux 新闻组中准确地提供您想要的信息。comp.os.linux.networking 新闻组就是通过提问寻找无线网络适配器驱动程序的好地方。在提出自己的问题之前，您最好看一看新闻组以前的档案，也许您的问题就解决了——如果他们知道您至少在尝试自己寻找答案，用户组通常更有帮助。在 http://groups.google.com 的 comp.os.linux 部分可以获得以前的问题和答案的归档文件。

Intersil 的 Prism 芯片组在许多品牌的大量无线网络适配器中泛使用。Intersil 的网站有当前 Prism 用户的列表，地址是 http://www.intersil.com/design/prism/Prismuser/index.asp。如果您的适配器使用了 Prism 芯片组，那么可以使用 linux-wlan 驱动程序，该驱动程序可以到 http://www.linux-wlan.com/download.html 中下载。

如果您的适配器不在 Prism 列表上，并且在前面提到的所有地方您都找不到所需要的 Linux 驱动程序，那么下一步就是确定您的适配器所使用的芯片组，并为该芯片组寻找驱动程序。您可以在联邦通信委员会的 FCC ID 搜索页面上(http://www.fcc.gov/oet/fccid)输入在适配器标签上找到的 FCC ID 码，基本上都能获得相关的信息。这个数据库提供了一个链接到另外一个存储档案副本的数据库，该数据库存有制造商为他们的应用程序填写申请的记录，通常包括技术描述以及一些电路图。通过研究这些文档，您就会知道适配器的芯片组是哪个厂家的，这就足可以使您找到所需的驱动程序。

7.3 其他 Linux 无线程序

某些特定无线适配器的 Linux 驱动程序提供了配置实用程序，这些实用程序可以控制通道分配、SSID 选择等。独立的无线应用程序包也可用于简化建立和使用对无线网络的无线连接的过程。

这些程序包中的一部分是基于目前绝大多数Linux版本都提供的Linux API无线扩展包，或者是基于使用无线扩展的无线工具程序。关于无线扩展和无线工具的组合文档可在以下网址找到：http://www.hpl.hp.com/personal/Jean_Tourrilhes/ Linux/Linux.Wireless.Extensions.html。

与其他 Linux 发表的无线软件一样，Linux 的无线工具 Web 页可能是了解信息的最好地方，地址是 http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html。

如果一个驱动程序支持无线扩展，那么用户在改变网络配置时就不需要重启驱动程序。无线扩展包在默认情况下是禁用的，用户必须启用内核配置中的 CONFIG_NET_RADIO 选项。

7.3.1 无线工具

无线工具 WirelessTools 是一组可以操纵无线扩展的程序。这些工具可以从 http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html 上下载。无线工具是命令行程序，但它们也提供了一个基础，从而使其他程序可以添加图形用户界面(GUI)来进行控制和统计工作。

无线工具包含一个/proc 条目和三个程序：iwconfig、iwspy 和 iwpriv。对最终用户而言，无线工具是易于使用的资源，但对于软件开发人员来说，它更像是一个框架。简单来说，它为其他程序完成实际的工作，所以有必要知道它的存在以及它做了什么。在实际操作中，除了最核心的命令行操作，每个人都可以很容易使用 KOrinoco 和 gWireless 这样的工具。

/proc/net/wireless

/proc 条目列在/proc 伪文件系统中，它用于显示某些无线接口的统计信息。该条目能作为一个文件来使用，所以您可以通过 cat /proc/net/wireless 命令来显示这些无线统计数据：

```
.....
>cat /proc/net/wireless
```

```
Inter - |sta|     Quality          |Discarded packets
face   |tus| link   level   noise  | nwid   crypt   misc
eth2:   f0  15.    24.     4        181      0       0
```

上面所显示的数据看上去很像密码，但却是可以理解的：

- 状态清单显示网络设备的当前状态。
- Quality 值显示链接的信号质量，接收器的信号级别，以及接收器在无接收信号情况下的噪声量。
- Discard 信息包的值显示因为一个无效的网络 ID 所丢弃的包数量，或者显示因为适配器无法解密包的内容而丢弃的包数量。

iwconfig

iwconfig 程序控制无线适配器的配置选项。一个 802.11b 的网络中包含以下参数：

- channel　适配器将使用的通道数。
- nwid　网络标识，在 802.11b 网络中，nwid 等同于 SSID。
- name　无线网络的类型或者在该网络中使用的协议名称，可以是适配器的类型，或者只是一个通用名称，如“802.11b”。
- enc　正在使用的密钥。

不带参数的 iwconfig 命令将产生当前所有 iwconfig 和/proc/net/wireless 值的列表。

iwspy

iwspy 程序设置并显示本地计算机的 IP 地址和 MAC 地址。

iwpriv

iwpriv 程序为设备特有的扩展特性提供额外支持。

7.3.2　KOrinoco

Korinoco 是适合于 KDE 图形化桌面环境的的程序，它以一组图形化显示和对话框使用来自于无线工具的信息和配置设置。Korinoco 模仿 Windows 平台下 Orinoco Client Manager。尽管这个程序看起来是随 Orinoco 网络适配器提供的，但它也可以供其他品牌的适配器使用(如果驱动器支持 Linux 无线扩展)。该程序的有关信息和下载提示可以在 http://korinoco.sourceforge.net 在线找到。

KOrinoco 的主状态窗口显示了当前连接的必要信息，包括信号强度、频道号和当前网络连接的 SSID。KOrinoco Configuration Editor 提供了与无线接入点关联或加入特别网络所必须的所有可选项。

7.3.3 gWireless

gWireless 是另外一组使用来自于无线工具的信息的无线程序。它包含一个会根据当前网络连接质量的改善而按照红色、橙色、绿色变化的 Gnome 面板小程序，以及由 iwconfig 命令控制选项和信息的图形界面。图形界面目前仍在开发之中，但这个项目是很有希望完成的。gWireless 程序相关信息的主页可以在 http://www.gwifiapplet.sourceforge.net 中找到。

7.3.4 NetCfg

NetCfg 是 Gnome 环境下的网络配置工具。它允许用户创建和管理连接配置文件，并实时地改变网络设置。NetCfg 的主页是 http://netcfg.sourceforge.net。

7.3.5 Wavemon

Wavemon 使用 ncurses 来监控和配置无线适配器的设置。它包含一个以图形化形式显示无线工具中所有重要信息的 Overview 屏幕，一个当信号强度低于预先设置值时触发的“级别告警(level alarm)”触发器，以及一个以全屏显示过去一段时间内信号级别、噪声水平、信号质量的历史记录。它同样有一个配置工具，通过使用菜单来简化设置过程。

要获取关于 wavemon 的详细信息并寻找最新版本的程序，可查看 http://www.jm-music.de/projects.html。

7.3.6 状态显示程序

有许多程序可以从/proc/net/wireless 列表中导入信息，并以图形方式显示。这些工具的主要区别只是显示格式上有所不同。

Wvlanmon

Wvlanmon 是另外一个 Gnome 面板程序，它可以使用彩色条显示链接质量。您可以在 http://tobi.tildesoftware.net/index/projects/wvlanmon 中找到它。

E-Wireless

E-Wireless 是一个 Enlightenment epplet，它可以通过/proc/net/wireless 列表的内容监控和显示信号质量的相关信息。该程序的在线地址为 http://www.bitshift.org/wireless.shtml。

Wmwave

Wmwave 是一个可停靠的应用程序，它通过屏幕上一个小窗口来显示链接质量、

信号级别和噪声级别等信息。该程序的在线地址为 http://www.schuermann.org/~dockapps/。

GKrellMwireless

GkrellM 监视器堆栈是一个以图形化显示系统信息的工具，它可以使用主题来匹配各种 Windows 管理器的外观要求。GkrellM 无线插件向监视器堆栈添加无线网络连接的有关信息。有关 GkrellM 的通用信息，可以在 http://web.wt.net/~billw/gkrellm/gkrellm.html 中找到。有关无线插件的详细信息，可以在 http://gkrellm.luon.net/gkrellmwireless.phtml 中找到。

WireStat

WireStat 以 Xload 格式显示无线网络连接。您可以在 http://www.bogor.net/idkf/idkf/software/linux-hack/wlan/中下载到相关程序。

7.3.7　远程监视

/proc/net/wireless 看起来像一个文件，所以它可以通过网络检索远程网络客户机的状态信息。Steven Hanley 的信号级别服务器和客户端程序能够以图形方式显示信息。要了解详细信息和下载软件，可以查看 http://wibble.net/~sjh/wireless。

7.4　配置接入点

除了 Apple 的 AirPort Base Station，绝大多数无线接入点的配置实用程序使用基于 Web 的接口，或者在远程终端上使用内置的命令行接口，或者是二者都有，所以当您使用主机连接到接入点时，使用任何操作系统都没什么区别。接入点的命令、控制方法和状态显示在任何系统上都是一样的。

Apple 的 AirPort Base Station 接入点却有一些不同的问题。AirPort Base Station 接入点提供的内置软件会假定您正在一台 Macintosh 计算机上进行配置工作，并且使用的是 AirPort Setup Assitant 和 Airport Admin Utility。

从一台 Linux 主机上安装 AirPort 基站需要一个 Linux 配置程序。目前只有一个程序，即 AirPort 基站配置程序(Airport Base Station Configurator)能符合要求。针对两个不同版本的 AirPort 基站(“Snow”和老版本的“Graphite”)的独立程序可以从 http://edge.mcs.drexel.edu/GICL/people/sevy/airport 下载。

因为是作为 Java 应用程序而编写，所以 AirPort 基站配置程序可以在任何安装了 Java 运行环境(JRE)的计算机上运行，包括 Windows、Solaris 以及 Linux 平台。您可以从 http://java.sun.com/products/jdk/1.2/jre 获得 JRE 副本。

第8章　Unix下的Wi-Fi

目前，对于使用各种类型 Unix 的用户而言，可供选择的无线接入方式是有限的，但是，它们的确存在。虽然 Unix 系统下的无线适配器驱动程序和无线网络软件比 Linux 系统少，但是对于将运行主流 Unix 版本的计算机连接到无线网络，仍然提供了足够的支持。在 Unix 中更为重要的是，您必须在购买适配器前获得合适的驱动程序，因为有些适配器的驱动程序并不适用于每个 Unix 版本。当然，对于 Orinoco，Cisco 这样广泛使用的内部芯片一般都是支持的。但是，如果您有一个杂牌的适配器，那么可能就不那么走运了。

8.1　Unix 驱动程序

如果您已经有一块无线适配器，并且希望能将其用于运行 Unix 的计算机中，那么您可以直接选择标准的驱动程序，或者可以搜索新闻组和邮件列表中的相关信息，从中找到适合现有 Unix 版本的驱动程序。网址为 http://www.freebsd.org/search/ search.html 的 FreeBSD 搜索主页就是一个特别好的搜索引擎，即使用户正在使用一种不同类型的 Unix，通过查询也可以准确地得知每种适配器应使用的驱动程序。当然，您也不难发现，最佳的解决办法就是购买其他品牌的适配器。

如果您还没有无线适配器，那么对于 Unix 用户而言，最佳的解决办法就是购买一块 wi 和 an 驱动程序所支持的适配器。当然，您也可以选择其他适配器，但是这种做法既费时又费力。每种 Unix 版本的主页都提供了使用 wi 和 an 驱动程序所需的准确语法及详细信息。

FreeBSD、OpenBSD 和 NetBSD 都为广泛使用的无线适配器提供了类似的驱动程序和相关实用程序。wi 驱动程序支持 Orinoco 适配器，以及采用了 Intersil prism 芯片组的适配器，包括来自 3Com、Samsung、SMC、Addtron、Linksys 和 Microsoft 的产品。an 驱动程序(由 Aeronet 提供，这家公司已经被 Cisco 兼并)用于 OpenBSD 下，它用于 Cisco 340 和 350 适配器。

您如果可以标识适配器中的芯片组，那么就可以指出应该使用的驱动程序。大部分情况下，用于适配器中的芯片组名称都会显示在提交给 FCC 的文件上。如果不清楚适配器中是何种芯片组，那么您可以使用 FCC 提供的在线 ID 号码查找工具，在 http://www.fcc.gov/oet/fccid 地址中进行搜索，您可以找到大部分适配器设计的技术细

节描述。

8.2　配置工具

每个 BSD Unix 版本都包含了相应的配置程序，您可以使用它们控制使用 an 和 wi 驱动程序的适配器的设置和选项。有些命令语句的名称会有细微差别，但是它们的功能基本相同。表 8-1 列举了不同 BSD Unix 版本的配置命令。

表 8-1　Unix 配置工具

Unix 类型	wi 的配置	an 的配置
FreeBSD	Wi wiconfig	不使用驱动程序
NetBSD	wiconfig	ifconfig 和 ifmedia
OpenBSD	wicontrol	ancontrol

随着 Wi-Fi 网络的普及，越来越多版本的 Unix 可以支持无线以太网服务。只要各种新驱动程序一出现，成为人们开始讨论的话题，相关的官方和非官方的邮件列表、新闻组和 Web 站点就会提供相关信息和网络支持。

wiconfig 和 wicontrol

用于 wi 驱动程序的配置程序可以设置所有网络和适配器选项。wiconfig 和 wicontrol 命令的语法在所有三种包含它们的 Unix 版本中都是一样的。

802.11b 网络中的 wiconfig 的语法是：

```
wiconfig [ interface] [-o] [-e 0|1] [-k key [-v1|2|3|4] ]
    [-t tx rate] [-n network name] [-s station name ] [-p port type]
    [-m MAC address] [-d max datalength ] [-r RTS threshold]
    [-f frequency] [-A 0|1] [-M 0|1] [-P 0|1] [-T 1|2|3|4]
```

wicontrol 的语法与上面完全一样。

interface 参数可标识网络适配器的逻辑接口名称。其名称一般为 wi0、wi1、wi2，依此类推。假如您的计算机只有一块适配器，则显示的名称为 wi0。

如果需要查看网络适配器的当前设置，可输入命令语句 (wiconfig 或者 wicontrol) 和接口名，并且不用加任何其他标记。但只有当您对系统进行根访问时，WEP 密钥才会显示出来。其他的选项见表 8-2。

表 8-2　wiconfig 和 wicontrol 选项

选　项	描　述
-o	显示该接口的统计数据
-e	启用或禁用 WEP 密钥，输入-e 0 关闭密钥，输入-e 1 启用密钥。加密的默认选项是关闭密钥
-k key [-v 1/2/3/4]	设置 WEP 加密密钥。如果不加-v 参数，该命令将设置第一个密钥
-T 1/2/3/4	指定适配器用于加密外发数据包的 WEP 密钥
-t tx rate	设置传输速率，tx rate 的取值如下： 1　1Mb/s 2　2Mb/s 3　自动选择速率(默认值) 4　4Mb/s 5　6Mb/s 11　11Mb/s
-n network name	设置客户机加入的网络名称(SSID)，默认设置是一个空字符串，该字符串将指示客户机关联第一个发现的接入点。-p 选项必须设置为 BSS 模式，该选项才能工作
-s station name	设置在网络中标识该客户机的名称
-p port type	标识该网络客户机将使用的操作模式。使用-p 1 表示基础模式，使用-p 2 则表示特别模式
-m MAC address	改变网络适配器的 MAC 地址，一般来说不要改变制造商设定的 MAC 地址
-d max_data_length	以字节为单位改变最大帧的大小。默认值是 2304
-r RTS threshold	以字节为单位设置 RTS/CTS 的阈值。默认值是 2347
-f frequency	设置适配器使用的通道号。在基础模式下，大多数网络适配器自动扫描所有可用的通道来寻找接入点，所以这个选项可以被忽略，除非您想在当前有多个信号的环境下指定一个特定通道
-M	启用或禁用该选项来减少微波炉的干扰。0 表示禁用，1 表示启用
-P 0/1	启用或禁用电源管理

上述功能说明看起来要比实际操作复杂。但事实上，如果操作系统内核可以识别适配器，并且如果适配器的配置符合接入点以及同一个网络中其他适配器的配置要求，则用户可以无障碍地进行连接。如果操作系统内核无法识别适配器，则必须重建内核。

当您新建一个连接时，使用单独的命令来输入每个选项要比运行包含所有选项的整行命令语句更容易操作。表 8-3 列出了经常使用的命令。

表 8-3　常用命令

wiconfig -p 1	将网络客户机设置为在有一个或多个接入点的基础模式下工作
wiconfig -s Sally's Laptop	将网络节点标识为“Sally's Laptop”
wiconfig -e 1	打开 WEP 加密功能
wiconfig -k [WEP key]	设置 WEP 加密密钥

除了使用无线设置外，用户也必须设置标准的网络配置选项，以便适用于任何 TCP/IP 连接。绝大多数 Unix 系统都提供 ifconfig 命令完成这些设置工作。

一旦完成了无线网络适配器和网络连接的配置，对它们的操作就和其他网络连接没什么区别。您可以运行网络实用程序，例如 ping、Web 浏览器、电子邮件客户程序和其他应用程序，对网络资源的连接就像正在通过有线网络运行并连接它们一样。

当然，您也可以直接从 Unix 平台上通过无线链接和同一网络中的其他计算机建立连接，而不用考虑远程计算机正在使用的操作系统。如果所有的计算机都接入相同的网络，则它们可以无障碍地交换无线电信号和数据。

8.3　Unix 下的实用程序

一些在前面章节中已有所描述的 Linux 配置工具和状态显示程序已经被移植到了一个或多个 Unix 版本中，但是用户仍然不像在 Linux 或者 Windows 下那样有太多的选择。原始的实用程序甚至更少，不过现在的 Unix 领域中已经有了一些这样的工具。

8.3.1　Xwipower

Xwipower 是一个以屏幕图标形式显示无线信号强度的实用程序，它还可以使用条形图实时跟踪信号强度。如图 8-1 所示，信号强度图标使用一系列条形图显示接收到的信号强度。该图标在适配器无法检测到信号时会使用日语显示一条信息(直接翻译过来就是“不在信号区域内”)。

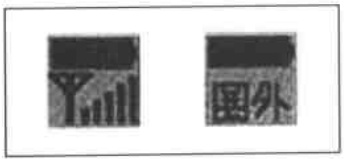

图 8-1　Xwipower 通过屏幕图标形式显示无线信号强度

图标同时也显示电池的容量。当图标中的小电池是实心时，表示电池容量为满，或

者计算机在使用外接电源。当电池容量低于 10%时，电池图标会变为空心。

Xwipower 在 FreeBSD 和 NetBSD 中工作，它可以从 http://iplab.aist-nara.ac.jp/member/ masafu-o/xwipower 下载。

8.3.2 WEP

WEP 是在 FreeBSD 中设置 WEP 加密的工具。它的下载地址和 Xwipower 一样。

8.3.3 bsd-airtools

bsd-airtools 是 BSD 的工具包，它用于检测和分析 802.11b 网络，并且控制基于 Prism 的无线适配器。bsd-airtools 包的主页是 http://www.dachb0den.com/projects/bsd-airtools.html。

bsd-airtools 包含以下工具：

dstumbler	在无线适配器的接收器范围中，检测和显示无线接入点信息的实用程序。
dweputils	审查和保护 WEP 加密网络，解密 WEP 密钥的实用程序集。
prism2ctl	Prism2 芯片组的调试模式(包括监控模式)的接口。
prism2dump	针对 802.11 网络流量的协议分析工具。

第9章　用于PDA和其他手持设备的Wi-Fi

Wi-Fi 网络并不局限于运行标准操作系统的标准计算机。现今，Palm、Handspring Visor、Pocket PCs，以及一些其他手持个人数字助手(PDA)都可以使用 Wi-Fi 链接与其他计算机进行数据同步，并且可以收发电子邮件和从互联网上下载数据资料。在不久的将来，一种混合型的设备就可以在具有广阔覆盖区域的相对低速蜂窝网络和只从接入点扩展几百码的高速 Wi-Fi 网络之间自动进行切换。

有些 PDA 在其他无线电服务中使用，例如 GSM 蜂窝电话网络(全球移动通信系统)，总之有一条原则就是，如果您所使用的 PDA 可以连接到传统的有线 LAN 上，那么就可以通过 Wi-Fi 链接进行工作。如果现在还没有合适的适配器，我们将在下文中向您介绍一款。

当您在离家或办公室很远的地方时，如果需要收发电子邮件，或者是在机场、咖啡馆甚至于大街上需要从一个公共热点进行在线信息查询时，具有 Wi-Fi 功能的 PDA 会特别有用。

9.1　在 Wi-Fi 网络中使用手持设备

在 Wi-Fi 网络中，支持笔记本电脑和台式机的网络结构对手持设备也可以提供同样的支持。一个或多个接入点像集线器一样用于无线网络，并且作为 LAN 有线部分和 Internet 的网桥。一个单一网络可以包括手持设备和大型计算机，因此完全可以使用无线链接来使 PDA 和其他计算机同步。

为了能够在无线网络中使用 PDA，PDA 必须有一个网络适配器、一个与适配器对应的驱动程序以及配置链接的工具。目前全球所使用的手持设备还没有一套通用的硬件接口标准，因此，每一种 PDA 都需要为其专门设计的适配器。

手持设备的形状可以各式各样，而且它们使用的都是有竞争的专用操作系统。因此，不可能存在一个标准类型网络适配器包(例如 PC Card)可以满足所有的手持设备。目前最通用的设计就是 CompactFlash 格式，尤其是在 Pocket PC 中，但是许多 PDA 需要专门设计的适配器或模块来满足它们自己的接口的需求。例如，Palm m500 使用的无线模块就无法在 iPAQ 或者 Handspring Visor 中使用。

将 PDA 连接到无线网络时，采用和建立与笔记本电脑或台式机链接相同的基本步骤：安装适配器，并且改变网络设置，从而使其符合所用无线 LAN 的要求。就接入点而言，PDA 只是一个网络节点。每个包中的数据格式都可能不相同，但这不是网络所关心的；它只是处理网络适配器在每个包的开头和结尾添加的帧。

9.2 Windows CE 操作系统

Windows CE 操作系统，以及最近的 Windows CE.NET 操作系统，都是微软为 Pocket PC、手持计算机以及嵌入式设备所提供的操作系统。目前广泛使用 Windows CE 操作系统的计算机包括 Compaq 的 iPAQ、Casio 的 Cassiopeia、Hewlett-Packard 的 Jornada 和 URThere 的@migo-600C。手持 PC 机比 Pocket PC 要大，但比传统的笔记本电脑要小。手持 PC 机的操作系统用于有着各种外形的计算机中，包括手写输入板和折叠的蛤壳式屏幕和键盘。最新的 Windows CE.NET 操作系统版本提供了对 802.11 网络的嵌入式支持。

对于 Windows CE 设备中的输入输出端口或插槽来说是没有单一标准的，因此无线适配器不可能全部进行互换。每一种型号(有时是每种模型)都需要与之相匹配的适配器。其中的一些使用用于笔记本电脑的 PC Card (采用不同的驱动程序软件)，而其他的则需要使用更小的 CompactFlash 适配器。表 9-1 列出了常用的 Windows CE PDA 和它们进行无线网络连接时所使用的适配器。

表 9-1　常用的 Windows CE PDA 和它们的无线网络适配器

制　造　商	型　　号	适配器类型
Audiovox	Maestro	CompactFlash
Casio	Cassiopeia BE300	CompactFlash
Compaq	iPAQ	CompactFlash 或 PC Card
Hewlett-Packard	Jornada	CompactFlash 或 PC Card
URThere	@migo-600c	PC Card
NEC	MobilePro	CompactFlash，PC Card 或两者
Toshiba	Pocket PC e 740	嵌入式

目前几乎所有的 Windows CE 设备都具备 USB 接口，因此它们都可以直接使用 USB 无线适配器连接到 Wi-Fi 网络中，但是，将一根 USB 电缆和一个比 PDA 本身尺寸还大的外置适配器挂到手掌大小的设备上是不切实际的。实际上，还没有一个制造商可以为 Windows CE 操作系统提供无线 USB 驱动程序，因此，这是一个不实际的方案。从

另一个角度来看，如果用户想将驱动程序或者其他软件加载到 PDA 中，那么 PDA 和其他更大的计算机之间的 USB 链接就非常有用。

您可以将 CompactFlash 适配器看成是 PCMCIA (PC Card)适配器的较小版本。CompactFlash 的尺寸大约如同火柴盒一般大小，它比 PCMCIA card 要小四分之一，但由于嵌入式天线超出插槽的边缘，所以无线网络适配器通常要略微大一些。另外，Intel、Kyocera、D-Link、Pretec、Socket 和 Symbol 都可以提供 CompactFlash 规格的 Wi-Fi 适配器。Symbol 的适配器如图 9-1 所示。

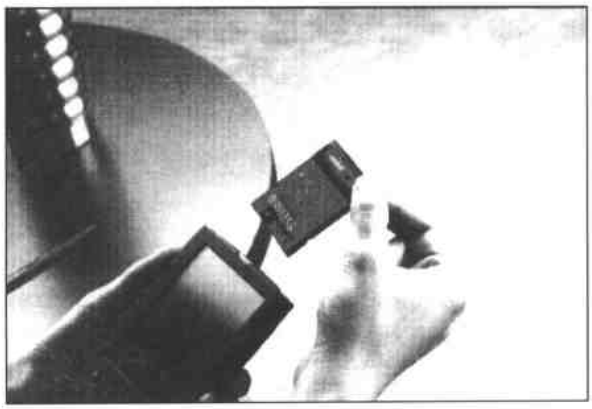

图 9-1　Symbol Wireless Networker 是一块 CompactFlash 适配器

更大些的 Pocket PC 包括由 NEC、Hewlett-Packard 和 Compaq 制造的产品，提供的是 PCMCIA 插槽，而不是 CompactFlash 插槽，因此如果您可以找到 Windows CE 的驱动程序，那么适用于笔记本电脑的 PC card 无线适配器也可以用于这些 Pocket PC 上。值得庆幸的是，大多数主流的制造商(当然也有一些小规模的制造商)都可以为用户提供 Windows CE 操作系统的驱动程序。建议用户可以到地址为 http://www.cewindows.net/peripherals/pccardwirelesslan.htm 的 Chris De Herrera 的 Windows CE Web 站点上查找最新的适配器及驱动程序下载链接。

如果您已经有了一个 PC card 适配器，并想在装有 Windows CE 的设备中使用该适配器，那么建议您去适配器制造商的 Web 站点中查找最新驱动程序。如果适配器制造商没有提供 Windows CE 操作系统的驱动程序，那么您可以在该适配器的背后查找相关的 FCC ID 号，然后通过地址为 http://www.fcc.gov/oet/fccid 的数据库运行号码，查询该适配器是否为私人版本，以及驱动程序是否可用。

安装和配置无线网络适配器

通常每种驱动程序都配有无线网络配置实用程序。对于不同的适配器而言，下载和安装新的驱动程序和配置软件的过程是不同的，但是通常都包含以下基本步骤：

(1) 将适配器插入 PDA。

(2) 将 PDA 连接到 Windows 台式机或笔记本电脑上。

(3) 使用 Microsoft Active Sync 实用程序将软件从较大的计算机传送到 PDA 上。在有些情况下，您必须先从制造商那里下载软件；除此以外，过程是一样的。

(4) 输入 PDA 与无线 LAN 和 Internet 连接的配置设置。如果 LAN 使用的是 DHCP 服务器，那么可以将 PDA 设定成自动接受 IP 地址；如果 LAN 使用的不是 DHCP 服务器，那么就需要手工输入为 PDA 指定的 IP 地址和网关服务器地址。

(5) 指定无线网络的 SSID，或者命令 PDA 检测并显示附近的所有 SSID。

(6) 如果网络使用的是 WEP 加密，那么就设置加密密钥。

(7) 断开 PDA 和计算机的电缆。

(8) 尝试建立一个网络链接，从而进一步测试网络是否运行正常。如果您的配置实用程序中包括了 ping 命令，建议您使用这条命令。

完成安装和配置选择操作之后，您可以选择 Start|Programs|Connections 并选择一个新的网络连接，前提是您的 PDA 必须连接到网络上。您也可以通过调制解调器或者有线网络运行所有同样的网络应用程序和配置实用程序。

9.3 Palm OS

Palm 手持设备和其他 PDA 的用户都使用 Palm OS 平台，他们并没有太多的无线选项。因为每种 Palm 手持设备都要求相匹配的网络接口包，因此与 Windows CE 操作系统相比，Palm OS 系列产品在无线适配器市场上并不具有吸引力。在 Windows CE 操作系统下，同一块 CompactFlash 或 PCMCIA 产品可以与多种不同设备协同工作。

Intel 的 Xircom 分公司为 Palm m500 和 m125 系列产品，以及 Handspring Visor 提供了 802.11b 适配器，而 Symbol 的基于 Palm 的 SPT 系列产品则已经嵌入了无线接口。Symbol 还获得制造 Palm OS 条形码扫描器的许可，该扫描器通过 Wi-Fi 网络将扫描的数据返回到主机上。然而，如果您有其他型号的 Palm 产品，或 SONY 的 Clie，那么您就不那么走运了。

9.3.1 Palm m500 和 m125

相对于通过蜂窝电话网连接的 Palm.Net 服务，802.11b 无线链接到 Internet 为用户提供了一个快速选择。Intel 的 Xircom 分公司为 Palm 手持设备提供的无线 LAN 模块代替了用于将手持终端设备连接到 PC 的标准 Palm 支架。当 Palm 与无线模块协同工作时，

用户可以使用 Wi-Fi 链接将 PDA 连接到主机上，从而进行 HotSync 数据交换和访问 Internet。图 9-2 展示了 Palm m500 的 Xircom 模块。

图 9-2　Xircom 无线 LAN 模块为 Palm m500 和 m125 提供的 snap-on 支架

通过 Xircom 适配器或 Symbol PDA 建立的 Wi-Fi 网络连接所使用的配置设置必须与所有其他无线网络客户端的配置一致。Palm 的客户端设置(例如 DHCP、WEP 加密、IP 地址等)必须与网络接入点的配置相匹配。

9.3.2　Handspring Visor

Handspring Visor 是另外一种 Palm OS 设备，它与 Palm 的手持设备采用完全不同的数据包。因此，它们不能使用相同的无线适配器。Xircom 的 SpringPort 无线以太网模块可以直接插入 Visor 顶端的插槽中；模块本身配有专用电池，因此，不需要增加 Visor 内部电池的功率消耗。

使用 SpringPort，您需要直接将模块插入 Visor 的顶端。Visor 将自动识别 SpringPort，并且显示一个有 5 个选项的配置屏幕：Client Settings(客户端设置)、Network Settings(网络设置)、HotSync Setting(同步设置)、Status(状态显示)和 Tips(提示)。

客户端设置屏幕中包含了配置选项，该选项用于在网络中标识 Visor 并建立链接。用户可以使用该屏幕分配一个客户端名称、指定网络的 SSID、启用或者禁用 WEP 加密和电源管理。

网络设置屏幕为用户提供了向 Visor 的网络配置中添加当前 SpringPort 选项的指令。

状态显示屏幕显示了当前链接的状态。它可以显示当前使用的两块电池(在 Visor 和 SpringPort 中)电量状态和信号强弱的状态。高级状态选项提供了 IP 信息和软件信息的选项菜单。IP 信息选项为用户打开了一个窗口，该窗口显示 SpringPort 当前的 IP 地址、子网掩码、DNS 服务器的地址、当前的 DHCP 状态情况和 SpringPort 的 MAC 地址。

9.4 其他手持设备

如果有谁正在为 Blackberries、Psions 或其他各种类型的 PDA 制作 802.11b 网络适配器，那么他们肯定会对此保密。当对无线 LAN 的需求不断增长，并且新的手持模型出现时，这种情况也许会改变。但目前许多模型甚至无法接入 Wi-Fi 网络，并且许多手持设备(例如 Blackberry 和其他一些 Palm)都被设计为用于使用其他无线服务的内置无线电，所以将 2.4GHz 无线电添加到同一包中是非常不明智的。其他手持设备的市场占有率非常低，而且即使有潜在的销售利润，也不可能弥补研发成本，因此制造商不可能花费人力物力去为它们研发 Wi-Fi 接口。

因此，您不可能将特殊的 PDA 随意地接入 Wi-Fi 网络。如果您不打算使用那些符合标准的终端设备，那么惟一的选择就是更换不同的 PDA 模型，或者是使用其他途径接入无线网络。当然，您最好也能意识到一点，那就是您根本不可能随心所欲，所以最好根据实际情况而定。

9.5 大不等于好

标准的 Palm OS 显示屏尺寸是 160×160 像素，Windows CE 的显示屏比较大(最大为 640×480 像素)，但是显示的物理尺寸要比同级别的笔记本电脑要小得多。因此，在常规显示器中看上去很好的图像显示在手持设备上却不一定很好。随着越来越多用于连接 Internet 的带有小型窗口的设备出现，许多 Web 站点和相关服务将会配合那些小窗口——当然，要想在尺寸只有几个平方英寸的窗口上看见在标准配置计算机窗口上所能看见的全部信息是不实际的，因此，PDA 的 Web 服务通常会使用专门为满足目标客户需求而设计的特定窗口。实际上，这意味着要为使用手持设备的用户提供成功的 Web 服务，就必须在每一个屏幕上严格控制各种数据资料，而不是采用大页面来迫使用户上下左右滚动页面。大量的嵌套页面是常见的解决方法。

正因为显示窗口不可能很大，而且大多数 PDA 被设计为在相对低速的网络连接下工作，因此，用户不要指望可以像笔记本电脑或者台式机那样的方式在线使用自己的 Palm 或者 iPAQ。网络的功能大多不同，但是内容却有很大不同。

9.6 远景目标

新一代的 Wi-Fi 接口将会比当前使用的 CompactFlash 适配器要小得多。SyChip 是

BELL 实验室的一个上市公司，该公司已经开始了一套为小型接口模块而进行的参数设计，这将会为蜂窝电话以及其他电器和设备添加内置 802.11b 功能。同时，一些公司已经开始研发一种新的“智能电话”产品，这种产品将把蜂窝电话、PDA 和 Wi-Fi 客户端的功能结合到一个袖珍的或袋装的包中。这些设备将允许当用户在 802.11b 热点范围内时建立一个高速 Internet 连接，而当蜂窝连接是惟一可用的无线网络接入时，则降为低速蜂窝网连接。其他产品可能将 Wi-Fi 和蓝牙技术相结合，提供与附近外围设备的无线连接。

值得注意的是，Wi-Fi 网络并不关心通过网络传输的数据种类或发送和接收数据的客户端设备类型。只要帧、信息包和无线电调制方法符合 802.11b 规范，网络就允许数据通过，所以，当前将笔记本电脑连接到互联网所采用的技术未来将出现在提供全新服务的嵌入式模块中。例如，家用电器、办公设备和汽车将把诊断信息传到中央控制中心，使用这些设备的用户发现问题之前，由控制中心诊断问题并派出技术人员进行修理。水表和电表将允许远程收集收费数据，而不需要在每一个测量位置上派专门的读表员。目前这些应用程序将很有可能选择使用蓝牙，而不是 Wi-Fi，但是我们也可能在今后几年中看见一些嵌入式 Wi-Fi 设备。

尽管存在着 3G 无线接入的竞争，Wi-Fi 以及后续产品仍会向广泛用于各种设备的目标迈进。

第10章 扩展网络

制定 802.11b 规范最初的想法是为诸如商店、家庭和公共机构等有限区域提供到局域网的无线连接。Wi-Fi 被认为是从传统以太网到笔记本电脑和无法使用缆线连接的计算机的简单扩展。其他无线电服务将能够提供从公共场所到 Internet 的无线连接。

不过，那只是一个计划。Wi-Fi 装置价格便宜，不需要许可证，而且安装和使用也相对容易，所以一个关于“游击网络者”的完整文化已经出现，并开始了由 802.11b 网络扩展到办公室、教室和家庭以外的替代技术的开发。业余爱好者和社区组织者在屋顶和山坡上安装天线，在那里他们可以为所有的邻居提供公有的或私有的到 Internet 的无线接入，还可以在几英里的距离之间创建点对点的数据链接。很多学院和大学都增加了校园网的户外无线接入点。一些城市已经开始建立最终覆盖全部市区的 Wi-Fi 网络。

这仍然是一个主要由激情的技术怪人和网络黑客推动的基础性运动。但是它却被认为是移动连接下一阶段价值几十亿美元的 3G(第三代蜂窝移动通信)无线网络的有力竞争对手。如果这些用管子套着的带子和咖啡罐里的天线匆匆拼凑起来的非商业性网络能够提供分布广泛的、可靠并且便宜的 6 Mb/s 无线网络接入的话，3G 蜂窝网的经营者将很难说服人们去购买他们昂贵的 384Kb/s 服务。因此，商业性的蜂窝网和无线网络的运营商们正密切关注着这种社区网络的动向。

安装和使用 Wi-Fi 网络，从而在建筑物之间传输数据或者在诸如您家的后院、停车场或其他开放的地方提供网络接入是一件相对比较容易的事情。户外天线很容易获得，如果您喜欢的话，也可以自己做。

本章包括在您的私有财产之外的地方管理和使用无线网络的法律的和实际的问题。并且还提供关于户外接入点和天线的技术资料。下一章您将学会如何使用 Wi-Fi 设备来创建和使用点对点网络链接。

10.1 法律问题

Wi-Fi 网络不需要许可证，但是 FCC(联邦通信委员会)和其他制订规章的代理机构已经建立了一些无线电传输规则，从而使这些网络得以实现。这些规则中的大部分极大地减小了无线网络与无绳电话及其他共享相同无线电频率的服务发生干扰的可能性，所以任何人都无法享有超越附近其他用户的特权。

当您尝试着建立一个具有最大可能覆盖范围的 802.11b 网络，而不是仅仅将建筑物

内所有的计算机连接起来的时候，接入点的无线电信号强度和网络适配器就成了更加重要的问题。信号强度与信号能传输的距离有着直接联系，所以，确切地理解规则所允许的内容非常必要。

针对美国境内的802.11b无线电设备的规则在FCC规则的第15部分，15.247节。以下是规则的内容：

(b) 定向的发射设备的最大峰值输出功率不能超过下面的规定：

(1) 对于[...]所有直序扩频系统：1瓦。

(3) 除了这一节的(b)(3)(ⅰ)、(ⅱ)和(iii)段情况之外，如果传输天线的定向增益超过6dBi，则定向的发射设备的峰值输出功率应该根据定向增益超过6dBi的dB数减小到本节的(b)(1)或(b)(2)段所标明的值以下。

(i) 如果天线的定向增益每超过6dBi 3dB，定向发射设备的最大峰值输出功率就减小1dB的话，那么工作在专门用于固定的点对点操作的2400~2483.5MHZ波段的系统就可以使用定向增益超过6dBi的发射天线。

上面的规则意味着什么？首先，这些规则允许无线电接入点和网络适配器处的无线电发射机的功率达到1瓦。其次，天线的最大增益为6dBi，除非在您提高增益的同时减小发射功率。相对于一到多点系统，具有高度定向的点对点系统允许使用更高的天线增益。天线的最大功率不能超过1瓦，但是您可以通过使用定向天线来使有效发射功率提高到4瓦。

如果严格遵守FCC(联邦通信委员会)规则的话，每个天线必须和您想要与它一起使用的特定接入点一起认证。这些认证可以从出售天线的公司得到。

当您计算无线电设备的输出功率时，必须同时考虑无线电设备和天线之间的电信号的损耗。例如，接入点的输出可能是20dBm(相当于略小于0.5瓦特的量)，但是连到天线的特定电缆在2.4GHZ的频率上可能会损失6dB。所以，天线将只能从无线电设备处接收到14dBm。这是少于1瓦特的量。从而就给天线增益留有余地。

在大多数Wi-Fi接入点和适配器中内置的无线电设备仅仅使用0.030瓦的功率传输信号，所以它们能够很好地适应法规的限制，除非您将它连接到有着极大增益的巨大的天线上。无线电设备和天线之间的RF(射频)放大器可能会使功率超过1瓦，当然，这将和FCC的规则冲突。

两种不同类型的Wi-Fi信号能从更大的发射功率中受益：对于点对点信号，增加功率可以增加两个站点之间的距离；对于一到多点信号，增加接入点的功率能够扩大覆盖面积，使更多客户端设备能够成功连接到网络。典型的点对点链接两端都使用高增益的定向天线；而在一点到多点系统中，接入点通常使用全向或扇形天线，以便能够覆盖比较宽广的区域，但是客户端适配器可使用定向天线。

无论如何，FCC对2.4GHz波段上的无线电传输设备的功率限制很严格。最好是能

够输入 5 瓦特的功率到高增益的天线，从而可以在五英里或十英里甚至更远的距离之间建立一个完整的可靠的数据链路，或者使用一个单接入来覆盖更大区域。然而，电话公司和其他销售数据服务的服务提供商对于规则的制定者有足够的影响力，使得他们保持着低功率的规则。因此，1 瓦的限制可能继续保留，除非在乡村地区。

作为一个负责任的守法公民，您应该总是严格遵守联邦政府的规则。作为一个负责任的守法作者，我决不怂恿您去做其他任何事。然而，个人或商业团体使用高增益天线来提高无线局域网的信号强度会引起 FCC 或其他执法机构注意的假想是极不可能的。除非这样的信号对别人的网络或无线电服务产生了很大的干扰，或者它吸引了本地电话公司或主要的 Internet 服务提供商的注意。而且，即使有抱怨，也很难确定非法信号的来源地(除非有庞大的天线在屋顶或建筑物旁边的空地上)。在 FCC 的功率限制下操作 Wi-Fi 网络是正确的，然而增加信号强度并不是难事。

通常，FCC 不会花费时间和资源地去关心对来自未经许可频率的干扰的申诉，像 Wi-Fi 网络使用的 2.4GHz ISM(工业、科学及医药设备)波段就属于这种频率。但是法律就是法律，因此作为原则来讲，持正当意图购买并且阅读这本书的人不会把增强接入点和网络适配器的功率或者使用很高增益的天线当成一件值得炫耀的事。

如果您在北美之外的地方阅读本书，请记住，FCC 的规则只在美国适用。其他国家的规则制定者已经设置了它们自己的限制，其中有一些甚至高于美国的标准，而且他们的强制政策可能更加严厉，所以在网络中安装高增益的天线或者射频放大器之前，向技术和法律方面的专家咨询一下是很重要的。

虽然大部分无线网络(甚至是带有高增益天线的网络)，其输出功率应该完全在安全范围之内，但是在您的附近操作高增益的或者放大的天线并不是一个好主意。许多接入点处都设有提示，警告不要在身体附近，尤其是眼睛附近操作设备。当使用放大器和高增益天线设备时，这一点应该牢记在心。

10.2　室外天线和接入点

Wi-Fi 网络中的接入点和网络客户机之间无线电链接的信号强度与下面几个因素有关：

- 天线增益
- 发射功率
- 天线高度
- 电缆衰减

记住，Wi-Fi 链接在两个方向上都传输数据：从接入点到网络适配器以及从网络适配器到接入点。所以链路上的天线和无线电设备必须既能发送又能接收无线电信号。幸运的是，天线的增益和定向特征对发送和接收是一致的，所以能够提高输出信号有

效功率的天线也能够增强接收机对微弱输入信号的敏感度。

室外天线还必须能够在它所运作的物理环境中长期使用。疾风可能会使定向天线偏离它原先对准的目标；堆积的冰雪会使信号减弱，并且增加物理支撑部件必须承受的重量；光照会引起塑料外壳的老化。所以，很多天线都被密封在天线罩里或其他提供额外保护的包装里。

2.4GHz 的天线有很多种形状和尺寸。一个全向天线可能只是一个几英寸长的单个元件，也许再加上外壳。做成 PCMCIA 适配器的天线甚至更短。最常见的定向天线是 yagi 天线(比屋顶的电视天线更小)，类似于烟雾检测器的平面天线，可以高达三英尺的抛物线形的反射镜，有极宽孔径角度的大面板。

802.11b 网络使用数字无线电信号，所以如果您用更小更便宜的设备交换足够多的信号的话，就没有必要使用更高功率的或是特别的天线，或者将天线放在屋顶上。如果一个具有中等增益的天线可以产生能被接收的信号的话，则使用更大的更贵的天线并不会使您的数据变得更好。而且小天线不会引起人的注意，这样可以避免邻居或地区代理机构的抱怨。

10.2.1 天线特性

无线网络设备使用同一个天线来发送和接收无线电信号。天线发送数据时比接收数据要处理更多的能量，但是它们的性能特征是一样的。一个天线在增加了发射信号有效辐射功率的同时也同等程度地提高了接收机的灵敏度，所以连接到 Wi-Fi 接入点或网络适配器的天线会同时提高在无线电链路上传输的两个方向上的无线电信号强度。用来确定天线性能的最重要的参数是孔径张角和增益。

天线的孔径张角是指当天线在该角度或弧度内时，其辐射或检测到的能量最大或灵敏度最高。例如，如果一个天线的孔径张角是 20 度，最大信号强度的“窗口”从天线的正面扩展到两边各 10 度。当一个无线电链路中的两个天线都不在对方的孔径张角内时，信号强度将会降低。图 10-1 说明了一对定向天线互相对准的效果。

很多接入点和大多数的网络适配器内置的天线都不是定向的，所以它们在各个方向辐射和检测信号的效果都是相同的。无定向天线(也叫全向天线)的定义中不包括孔径张角的定义，如果有的话，应该是 360 度。顾名思义，点对点链接中的天线是直接互相对准的，所以它们的孔径张角可以很窄。

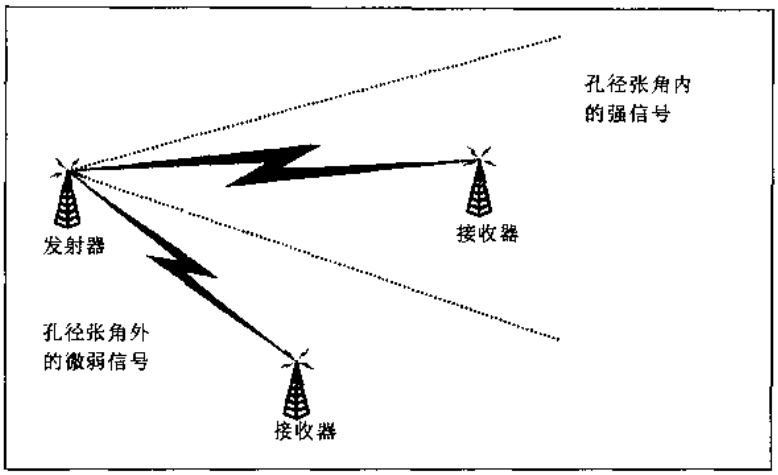

图 10-1　定向天线能够通过将同样数量的能量集中到更小区域来提高信号强度

天线的增益是它的有效输出功率或灵敏度相对于标准偶极天线的值。所以，如果测量从两个同样的发射器输出的信号或是相同的信号经过两个单独的接收器的同一信号的强度的话，通过 3dBi 增益的天线的信号将会比作为参照的偶极天线的信号强 3dB。当天线尺寸增加，或信号集中在狭窄孔径张角之内时，天线的增益将增加。

将天线的孔径张角和增益想象成聚集的光线会有助于您的理解。一个标准的灯泡在所有方向上散射同样强度的光线(除了灯泡的底座)。然而，如果您在光源的一边放上一个反射器，或者您将光线朝某一特定的方向聚焦，在目标区域光线的亮度将会明显增加，而在目标区域之外的地方将会变得更暗。灯泡发射出的光的总量是相等的，但是更多的光被集中到指定的地方了。

无线电设备的天线与之工作原理差不多相同。一个全向天线将向各个方向辐射相同的能量，而定向天线能够将更多的能量集中到某些方向。

小孔径张角的定向天线可以用在点对点链接上，但这并不是它在无线网络中的唯一用途。当信号与其他无线电信号有潜在的干扰问题时，使用定向天线并使其孔径张角的轴线偏离干扰源常常是有效的解决办法，这样接收天线就会对所需信号更敏感，而对干扰源不敏感。如果您想让网络覆盖您自家的范围，限制泄露到领居家的信号，您可以在您想要覆盖到的区域的边缘处放置一个或多个定向天线，并使其朝向里面。

具有更大表面积的天线比小天线更有效，但天线的实际尺寸也是极其重要的。对于某一频率的无线电波来说，其理想天线的长度应该等于该频率无线电波的波长或波长的倍数或波长的几分之一。所以在您的 802.11b 网络中采用经过特殊设计的工作在 2.4GHz 的天线是很重要的。长度适当的天线远比长度随意确定的天线更能有效地发送和接收 Wi-Fi 信号。

10.2.2 功率

802.11b 无线电发射器的最大功率由无线电设备的设计所决定；网络操作人员通常不能调整它，即便能，也不过是在高功率和低功率之间作一个选择而已。不过，可能有某个无线电设备的输出功率比法定的最大值低很多。因此常常可以提高到达天线的功率而不触犯法律。

由于您通常不能提高发射器产生的功率，那么提高接入点或网络适配器中无线电设备的信号功率的唯一途径就是在无线电设备和天线之间增加一个称为 RF(射频)放大器的设备。可认为射频放大器是一个黑盒子，它的输入是一个低功率的信号，它的输出是一个和输入信号内容相同的更强信号。

有的射频放大器可以按照在室内使用的要求设计，放置在靠近接入点、路由器或网络适配器的地方，其他的安装在室外靠近天线的铁塔或桅杆上。室内放大器通常很容易安装和维护，它们也很容易与交流电源相接，但是由于连接到天线的馈电电缆较长，吸收了放大器产生的一部分射频功率，所以它们的效果要差些。安放在天线附近的抗风化包装里的放大器可供给天线更大功率，但是要维修或替换它将变得很困难。如果您确实要使用室外放大器，最好使用能够通过天线馈电电缆获得直流电源的放大器。

HyperLink Technologies 公司和其他制造商提供在 2.4GHz 中使用的射频放大器。大部分放大器都是既能够放大从内到外的信号，又能够放大从外到内的信号。这是一个很有用的特性，使我们只要在链路的一端安装一个放大器就可以同时增强两个方向的信号。

10.2.3 天线高度

2.4GHz 的无线电信号沿视觉路线传播，因此您可以通过提高一个或两个天线的高度来增加信号传输的距离。这就是为什么人们常常会将无线电设备的天线放在屋顶、山顶和高楼上的原因。为了抵消地球表面曲率的影响，当信号传输距离增加时，两个天线的平均高度必须增加。

无线电波的“视线”实际上比两个天线之间的可视路径要宽。无线电波在环绕发送天线和接收天线之间直接路径的雪茄形状的区域内传播，这个区域被称为菲涅耳圈(读成 fru-NEL)。为达到最好传输效果，菲涅耳圈周围必须没有山丘、树木、建筑物和其他障碍物。

因此，无线网络信号的最大传输距离取决于两个天线的平均高度，同时要考虑到地球曲率和具有无障碍要求的菲涅耳圈的影响。表 10-1 列出了 2.4GHz 时各种距离所需要的最小估计高度。请记住，这些只是估计值，实际上您可能会将您的数据传输到更远

的地方。

表 10-1　天线高度和最大信号传输距离的关系

距　离	平均天线高度
1 英里	13 英尺
3 英里	27 英尺
5 英里	35 英尺
8 英里	48 英尺
10 英里	57 英尺
15 英里	83 英尺
20 英里	115 英尺

需要注意的是，两个天线的高度是在一般地形之上的平均高度；如果一个天线比平均高度越高，另一个天线就可以越接近地面。所以如果一个五英里长链路的一端在山坡或者在八层楼的楼顶上，则当两个位置之间没有障碍物时该链路另一端可以接近地面。

当您试着将 Wi-Fi 网络覆盖到一个大的区域时，更有效的方法是把接入点的天线放得尽可能的高，而非花力气去增高个别客户端的天线。

10.2.4　电缆衰减

将无线电信号从无线电发射机发送到天线，或者将其从天线发送到接收机的电缆并不是很有效的传输介质；每英尺电缆都吸收少量的但可测量的功率。这意味着当电缆长度增加时到达天线的功率将会减小。

对于短电缆，这种衰减的影响通常并不大，但是，对于长电缆可能会引起巨大的差异。如果天线在塔上或屋顶上，或者估计一个长距离的点对点链接所需要的天线增益，就必须在计算到达天线的信号强度时考虑到电缆的损失。对于某种特定类型电缆的损耗量取决于电缆的直径和材料。每种类型电缆的规格中都会包括衰减的大小，用不同工作频率下每 100 英尺衰减的 DB 数表示。

如果在 2500MHz 时，电缆衰减为 6.80dB，就可以估计出 20 英尺的电缆在 2.4GHz(2400MHz)处将会损失大约 1.3dB。如果接入点或网络适配器的输出功率是 20dBm，则通过该电缆天线将接收到 18.7dBm。所以当您将信号送到增益为 6dBi 的天线时，有效辐射功率的大小就是 24.7dB(20 - 1.3 + 6 = 24.7)。

电缆损耗随馈电电缆长度的增加而增加，所以应尽可能地把接入点和网络适配器放在靠近天线的地方。如果天线安装在屋顶或建筑物的墙上，就尽量将无线电设备放在

附近的设备橱里或是其他能够连接到交流电源和以太网电缆的地方。将连到接入点的以太网电缆加长从而缩短天线馈电电缆是比较有效的方法。

安装天线馈电电缆的时候，在电缆的两端都稍微放长一点是一个好习惯，这样在将电缆连接到天线和无线电设备或拆开连接的时候比较方便。但是不要因为预先做好的电缆超过您所需要的长度就在地上将这些电缆缠绕起来。因为所有的电缆都在消耗信号，并且没有任何益处。

10.3 校园网

通常，校园网为两个或更多建筑物内的用户或者围绕那些建筑物的户外的用户提供到 Internet 的无线接入，有时候也提供到 LAN 的无线连接。“校园网”存在于学院或大学的校园内，但同样的计划和设计也可以应用于其他地方。譬如，校园网可用于办公区域，工业园区，以及像公园、购物娱乐中心这样的公共场所，甚至还可用于农场或码头。有些城市已经安装了类似校园网的网络以便在它们的中心商业区提供公共的 Internet 接入。另一种形式的临时的类似校园网的网络在特别事件如音乐节、男(女)童子军大会或旧式汽车狂热者的集会进行时可能会建立。

最简单的校园网是偶然间产生的：从建筑物内部提供网络服务的接入点发射的无线电信号并没有在墙壁处停止，所以在停车场或是后院的用户也能建立到网络的无线连接。一个更大更复杂的校园网可能拥有额外增加的接入点，这些接入点被特别选定在大学的草地或是沿街的咖啡店等地方。

校园网可以是连接两个或多个建筑物到同一网络的一系列无线链接的补充，但是它们有本质上的区别：校园网应该能够覆盖大范围的室外场所，而点对点链接只是将单一的 LAN 扩展到几个建筑物的内部。本书第 11 章将详细介绍了关于设计和使用点对点网络链接的内容。

10.3.1 建立校园网

通常应用于设计一幢建筑物内的 Wi-Fi 网络规则也可用于校园网。为您的接入点选择位置以使它能够覆盖到尽可能多的地方，并且允许一个接入点的覆盖面积和与它相邻的每一个接入点的覆盖面积有百分之二十的重叠区域。每个重叠区域应该使用不同的无线电频道。

在很多情况下，用于室外网络的接入点都必须有连接器用来连接外部天线，而不是使用很多接入点自带的仅供室内使用的天线。根据您的特定需要选择具有最佳特性的天线，然后用一根电缆将它连接到接入点，接入点要放在不受风吹雨淋的地方。

1. 将接入点连接到 LAN 和 Internet

如果接入点都放在已经开通网络服务的建筑物内部，那么就可将接入点和室外天线看成是已有网络的简单扩展。如果您还没有将接入点连接到网络，就需要建立一个连接了。

为了将校园网连到 LAN 或 Internet，您必须让每个接入点都以某种形式连到网络。可以通过以太网电缆(从电信公司租借的数据回路)连接，或者使用点对点无线电链路。

每个接入点都需要电源，但并不是必须从附近的交流电源插座拉一根线过去。很多接入点制造商提供“以太网供电”的选择使得接入点可以通过传送以太网数据的电缆获得电源。

以太网线很容易连接到接入点，但是除了某些特定场合之外，这并不是建筑物之间链接的最好选择。首先，您必须有让电缆通过的安全路径；您不能仅仅将电缆缠在树上或者让它穿过草地。在校园里，有时候可以让电缆穿过小河或其他公用事业的通道，但在其他很多地方这是不实际的。而且即使您可以将电缆从一幢建筑物连接到另一幢建筑物，10Base-T 或 100Base-T 双绞线所允许的最大距离也只有 100 米。如果您的接入点在网络集线器 100 米之外，您就必须增加一个或多个中继器或用光纤代替双绞线。无论哪种方法，造价都可能高于使用无线电链接。

有时候接入点的理想位置在一幢已有 Internet 服务的建筑物内，但那不是您想要用来组建校园网的 LAN 的一部分。这种情况下，可建立一个虚拟专用网(VPN)链接，从 Internet 到您的网络创建一个“通道”。接入点将会通过 VPN 与您的网络传递数据，就像通过短电缆连接一样。

第三个可选方案通常是最实际的。使用点对点无线链路连接网络集线器和每一个远程接入点。为此目的而专门设计的室外路由器和相关硬件及软件可从 Orinoco，D-Link 以及其他许多供应商处获得。在下一章您可以找到关于点对点链接的详细信息。

2. 您的发射区有多大

每个接入点都使用最大的覆盖面积对于无线网络来说并不总是最好的设计。这就像蜂窝电话系统一样，网络接入的需求量决定了所使用带宽的大小。在有很多用户的地方，比如图书馆阅览室就可以使用两个或多个重叠的接入点，而只是偶尔有些用户的地方，例如停车场，可以只放一个接入点。当您设计自己的网络时，可根据不同天线的定向特征和增益来找到每个位置理想的平衡点。

3. 公共还是私有

校园网的访问权可以限制在运行这个网络的社区成员内，也可以对无线电信号范围之内的每个用户开放，或者可以配置成允许任何人连接到 Internet，但不允许连接到其他本地计算机的网络。例如，学院的网络管理员可能要为学生、教员和全体职工提供

接入校园的无线 Internet，而并不想提供给公众。另一方面，商业公司可能想为雇员提供不受限制的 Internet 和企业网访问权，但只允许参观者连接到 Internet。

控制到校园网的访问与控制到其他无线网络的访问没有区别——所有在室内网络中使用的工具都可以将非授权用户排除在网络之外。这包括 WEP 加密工具和接入点具有的 MAC 地址过滤功能，以及外部防火墙，它在允许用户接入网络前要求用户输入帐号和密码。

10.3.2 使用校园网

对网络用户而言，校园网和其他任何 Wi-Fi 网络一样，计算机中的无线网络适配器首先检测到无线电信号，如果它能识别 SSID 和其他安全选项的话，就建立一个链接。一些校园网只提供接入 Internet，而其他一些还提供到 LAN 或 WAN 的本地连接。

如果您的计算机没有获取到足够强的信号来建立网络链接的话，可以试着移动到别的地方。小型障碍物比如树木、建筑物墙壁的反射信号以及其他建筑物可能会干扰您的计算机和最近的接入点之间的双向信号路径。不过也许只需将计算机移动一两英尺就可以获得极大的改善。

10.4 组建邻域网

您可能会想到在相对简单的基于家庭的无线网络和复杂的校园网之间扩展家庭网络或者小型商业网络：您可以和附近的邻居共享高速 Internet 连接，或者允许您的雇员拿着他们的膝上型计算机去隔壁的咖啡店。如果您或您的小孩喜欢和隔壁邻居玩多人游戏，或者您想在年度街区聚会上和邻居闲聊时用掌上型计算机或袖珍型个人计算机上网，这时候邻域网可能是最好的选择。

在您决定在屋顶上悬挂天线之前，先考虑清楚用邻域网实现什么，如何维持网络其他部分的安全。如果您准备给网络增加一个特定的场所(例如某个邻居的房子或事实上已经成为您的部门办公室的咖啡馆)，您可以使用定向天线将信号集中到您想到达的特定场所。另一方面，如果您想在半个街区或更大范围内提供 Internet 热点给每个人，您可以在您的楼房的的最高点上放置一个高增益的无定向的天线。如果您将同一个 LAN 同时用于家庭和邻域网的话，一定要使用防火墙以使您的计算机同网络的公共部分分离开来。

如果您的网络适配器有一个用于连接外部天线的连接器的话，您可能想买一个或者做一个定向天线，以指向社区网络最近的接入点。使用它，您很可能会发现适配器内置的低增益全向天线检测不到附近的信号。我们将在下一章讨论如何制做天线。

10.4.1　让您的 ISP 高兴

与邻居共享高速电缆调制解调器或 DSL 服务，并且分担费用，或者让您的公寓或郊区的每个人都共享同一个连接，这些似乎是极好的主意。

但是考虑一下这对您的 Internet 服务提供商造成的潜在的恶化因素，他们可能会认为您慷慨的提供电缆或 DSL 帐户的共享是对他们(现实的或潜在的)财源的一种威胁和对服务条款的侵犯。一些主要的 ISP，包括 AT&T 宽带公司，SBC 和时代华纳有线公司，都有特殊的政策，不允许客户通过邻域网共享连接。很多其他的 ISP 并不关心甚至鼓励这样做。

ISP 关心邻域网可能产生超过他们预期的网络需求是有道理的。当您设计或构造一个通信网络时，您会根据预期峰值需求计算最大容量。如果计算正确，网络就会有足够的容量处理紧急情况，但是如果需求超过了您的预期，整个系统就会过载，从而必须增加容量。

这种设计同样应用于电话系统、高速公路和有轨电车线路，还用于 Internet 连接。如果您有足够多的有轨电车(或带宽)去处理繁忙时刻的交通，系统就可以有效地运行，收费箱里的钱应该能够支付您的费用。但是当线路的一端开了新的大工厂时，立刻会有 500 多个乘客同时要求使用您的系统，除非增加更多容量，否则电车就会非常挤，每个人都会抱怨。

经验可以让您精确地了解某一时刻有多少需求——您也许不能确切地知道星期二早晨 10：15 谁在线上，但是您可以预测需要多少电车或带宽来处理总需求。

对于 Internet 帐户的情况，ISP 已经建立了足够的带宽来处理峰值的需求。然而如果需求加倍了，它就必须购买并安装更多的设备，然后再想办法支付费用。自然，它想阻止会造成整个系统崩溃的额外的带宽需求，或者更准确地说，它想知道这个额外的需求，并执行相应的计划(和收费)。

所以您有两个选择：或者询问您的 ISP，是否有关于共享连接的政策，遵循它的条款(或者找其他的 ISP)；或者直接安装邻域网接入点，希望电话公司，电缆服务商或其他 ISP 不会发现它。

10.4.2　网络安全：每个人都是您的邻居

邻域网的最简单的配置是用一个单一的具有很宽覆盖范围的接入点提供不受保护的 Internet 连接。任何一个在信号范围内拥有网络适配器的人都能使用您的网络通过 Internet 交换数据。这不仅包括您的邻居家，还包括街边的货车里正在用您的网络下载色情图片的家伙。除非您想为每个路过的人创建一个公共的 Internet 热点，否则您至少

应该使用 802.11b 规范中的一种安全工具：

- 启用 WEP 密钥加密功能。一个潜心专研的入侵者确实能够在一小时内破解一个 WEP 密钥，但是这会使非专业的用户气馁。
- 使用 MAC 地址过滤功能来将您的网络访问限制在特定的网络适配器中。当然，用适当软件来产生欺骗性的 MAC 地址并不困难，但是这对于未授权访问又多了一重阻碍。
- 关闭给每个客户机自动分配 IP 地址的 DHCP 功能。给每个授权用户分配一个特定地址。
- 在您的接入点或路由器上开启防火墙功能。
- 使用一个外部服务器或其他防火墙来迫使每一个用户在连接到 Internet 之前提供用户名和密码。
- 使用虚拟专用网(VPN)。

如果使用同一个网络去连接两个或更多个计算机，应使用防火墙来将网络的这一部分与公共接入点隔离开来。还有，鼓励网络的合法用户密切关注文件共享操作，这样他们就可拒绝网络外部用户读写他们计算机上的数据。

最后，要确定更改接入点的管理密码，不要使用 admin 或其他任何一个广泛使用的默认密码。闯入接入点的入侵者会给您的网络带来巨大损失。

第11章　点到点链接和中继器

使用无线电设备来扩展局域网并不是一个新想法。用于添加网络远程客户机的设备和软件已经出现了至少十年。学校、商业公司、学术研究者和 Internet 服务提供商都使用扩频无线链接来将局域网和 Internet 服务扩展到传统有线网络不能覆盖的地方。但是费用和过程的复杂性使得这成为专家和奢华顾问们的工作。

由于低价的 Wi-Fi 设备已经比较普及，很多用户想到过将天线对准附近的建筑物或五到十英里外的山坡来创建一个便宜而高速的数据链路。一些实验者和时间多于金钱的修补工曾经用锡杯、炸土豆片的金属罐和地下室里车间里的废料设计出他们自己的天线。他们普遍发现 Wi-Fi 链接是在很多地方传输数据的可靠方法。本章包含了设计和使用点到点无线网络链接的内容。

一个点到点无线链接可以是一个大的 Wi-Fi 网络的一部分。它可以在两个有线局域网之间充当简单的网桥，或者为已有的局域网添加一个单独的远距离站点。点到点服务不同于其他 802.11b 网络，因为它在两个特定位置之间传输数据而不是广播网络信号到信号范围内的任何网络客户端。也可以将 802.11b 链接用作无线网关的一部分，提供 Internet 接入给地面通信线路到达不了的社区或单独的位置。

为什么要扩展无线网络？点到点链接可以达到以下几个目的：

(1) 它们可以将单一的网络扩展到将多个建筑物内的用户包括进来。在办公场地、大学校园、商业公司及学术部门等有不止一个建筑物场地的机构中，可以使用无线链接，来共享本机构场地之间的局域网服务。

(2) 它们可以穿过诸如高速公路或河流这样的障碍物来传输数据。如果有一条无障碍的视线的话，无线链接就可以跳过两栋建筑物之间无法布线的间隙。

(3) 它们可提供局域网和高速 Internet 接入给远程的用户和单独的计算机。无线链接可以将宽带连接扩展到宽带 DSL、电缆调制解调器 Internet 服务甚至普通的电话服务都没有覆盖的地方。

(4) 它们可以建立并不昂贵的无线网络链接来替代租用线路。电话公司提供的私有数据回路或其他通用载体通常会包括一次性的安装费和每月的月租。一条租用线路每年的费用常常是购买和安装无线链接的一次性费用的好几倍。

从某种意义上说，802.11b 点到点网络链接是与无线局域网完全不同的种类。虽然两者都使用同样的无线电技术，并且可以不受单个建筑物的限制扩展无线网络，但是点到点链接可以容易地在其他频率上使用其他类型的无线调制方法执行同样的功能，而不是 2.4GHz 上的 DSSS。您可以在本章后面找到将远程站点连接到网络的多种方法

的指示。

11.1　扩展局域网

一个点到点无线网络链接可以是一端连着局域网而另一端连着单个客户端设备，也可以是两个局域网之间的网桥。换句话说，一个链接的端点可以是一个单独的计算机，也可以是其他设备或整个网络。

包含一个远程客户端的无线局域网和在一栋建筑物内有两个或多个接入点的网络按照同样的方式工作，如图 11-1 所示。惟一的差异是一个或者多个连接到局域网的接入点使用室外天线对准远程位置的客户端计算机。远程计算机对网络来说和该网络上的其他每个计算机完全一样。

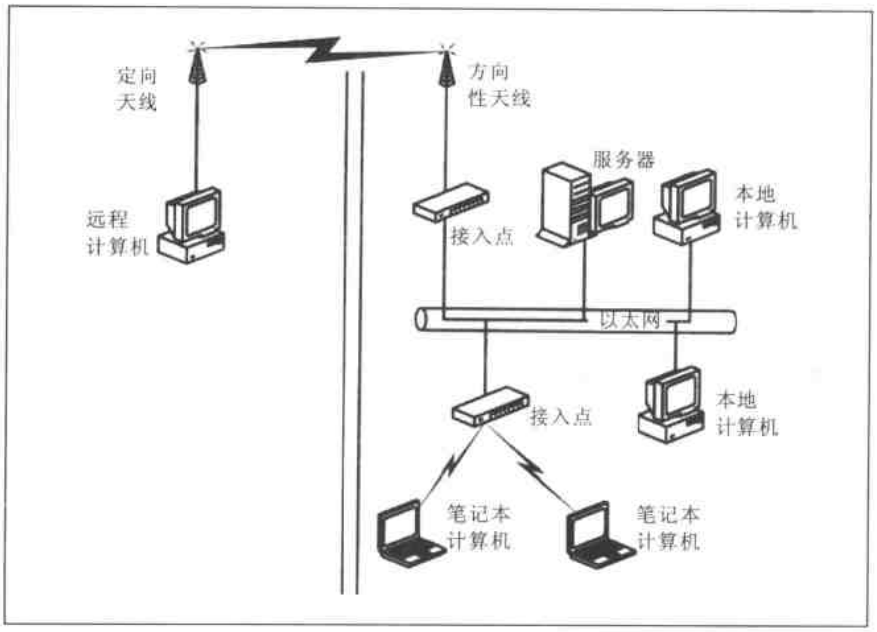

图 11-1　点到点无线链接能连接到远程位置的单个设备

无线网桥是同一局域网两个网段之间的链接，如图 11-2 所示。两个网段之间可以短到几百英尺，也可以长到几英里或更长。

如果两个端点之间的距离对于一个无线链接来说太长，或者在信号路径的视线上有障碍物的话，可以在点到点链接的源端和目的端之间的中继站上添加一个或多个中继器。中继站可以在独立的位置上，比如无线电发射塔或屋顶，或者在可能有额外的网络客户端的地方。例如，两个端点之间的第三个建筑物。

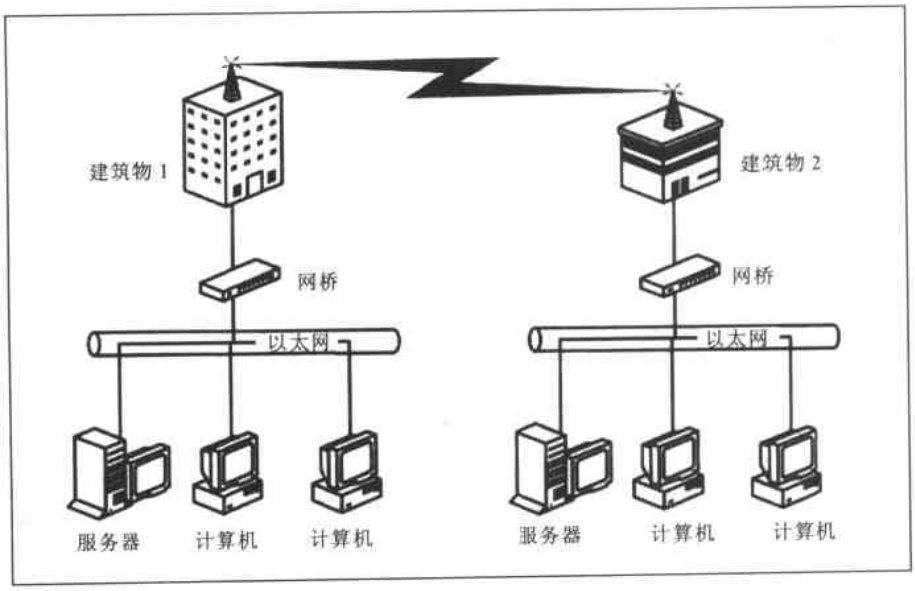

图 11-2　无线链接可以将局域网扩展到两个或多个建筑物

点到点链接可以使用任何带有外部天线连接器的接入点和网络适配器。不过，有几个厂家提供特别为室外网桥应用程序设计的无线路由器，并且这常常是一个更好的选择。Plexus、HyperLink、Orinoco 和其他厂商生产的路由器都整合了接入点的功能，因而可以使网络更容易组装。

11.2　点到点和点到多点

室内接入点或者使用全向天线从预期的覆盖区域中间向所有方向辐射同等的能量，或者将宽孔径张角的定向天线放在预期覆盖区域的一边或拐角处。接入点为指定区域(比如办公室或房子)内的任何位置提供无线服务，称为点到多点服务。它可以同时和许多网络客户端交换数据。

点到点链接有着不同的目标：它在两个固定位置之间传输尽量大的辐射信号。无线电信号在链路的两个方向上传输，所以每个接入点、路由器或网络适配器都用同一天线发送和接收信号。因为目标是将无线电信号集中到链路另一端的天线，所以至少要有一个端点使用定向天线。如果链路横跨了较长的距离，则两个天线都应是定向的，以便获得尽可能最强的信号。

在校园或类似区域，网络连接了若干个建筑物，网络链接可以被分割成从中心位置到多个方向远程站点的分布式网络服务。在这种系统中，中间的接入点使用无定向天线，每一个远程站点使用定向天线，如图 11-3 所示。两个远程站点大致在同样方向的时候，最好的选择应该是用一个具有宽工作角的定向天线。更复杂的系统既包括定向

天线又包括全向天线。

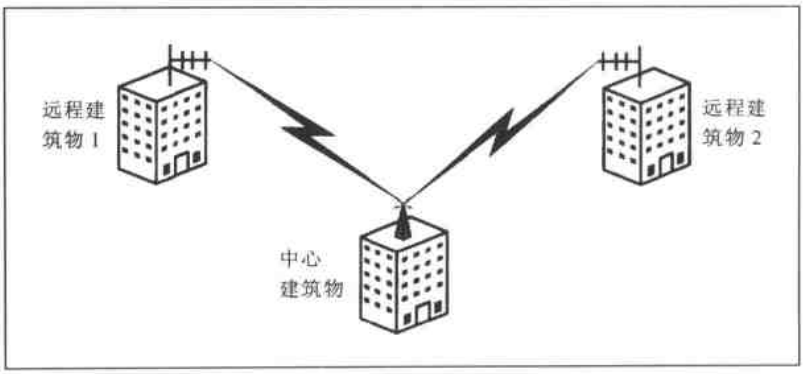

图 11-3　全向天线能同时将信号分发到两个或多个远程位置

11.3　安装点到点链接

点到点位置勘定的第一步是确定一条可能的信号路径。理论上，计算两个天线的高度，并且确定两者之间的路径应该是可行的，但是几乎从来不这么做。在您可以使用无线电并开始通过网络传输数据之前，几乎总是免不了要将天线扭来扭去。您可以预先用一张好的地图(例如，美国的地形图，地质勘测等)进行测量。但是在某些点，您可能想爬上屋顶(或从窗户往外看)来确认到您想要放置链路另一端的地方有一条视觉路线。如果路径有几百码长，您应该带一副望远镜。

您通常可以在没有任何特别允许的情况下在您自己的建筑物内放置天线，但是如果想使用商业性建筑物的屋顶的话，您可能需要获得财产所有人和本地分区规划委员会或其他土地使用机构的许可。如您正在安装一个不显眼的天线，这可能不是一个问题，但是如果您不得不使用相对比较大的反射器或类似的东西，您应该记住这一点。如果您使用现成的柱子或塔来安装天线的话，您必须确信没有对附近其他天线产生干扰或者被它们干扰。

系着装满工具的腰带爬上柱子或塔，将一个庞大的天线安全而精确地安装到 30 英尺或更高的空中可不是随便的午后计划。应考虑适当的安全设施，包括给每个人配安全帽了——一个掉下来的扳手或螺钉都可能是致命的。如果您对这方面工作没有经验，就不要羞于雇佣一个人来为您做这件事。出售这种点到点天线的人会告诉您哪儿可以找到合格的天线安装人员。

11.3.1　选择信号路径

安装链接的第一步是要精确地确定它通向什么地方。如果您只想将网络延伸到停车

场或高速公路对面，路径就是很明显的；选择一个位置确保建筑物前没有大树即可。但是如果链接超过半英里，您可能需要先在地图上画出来了。

纸上或者网上的地形图会给您最详尽的细节情况。http://www.topozone.com 处有全美国的地图；http://toporama.cits.rncan.gc.ca 是加拿大地图的出处。如果两个端点的确切位置不能立即在地图明确地标出，GPS(全球定位系统)设备能够提供精确的地理坐标。

11.3.2　到达偏僻地区：长距离链接

大部分点到点无线网络链接覆盖的距离可能是用码而不是英里来测量的，所以安装链接相对容易。链接的另一端在清楚的视力范围内，因而天线可以容易地互相对准。对于短的跃距，信号强度通常不是问题，尤其对于定向天线更是如此。

越长的链接越困难，因为信号会更弱，而且将天线精确地对准也更难。图 11-4 说明了为什么当您离开发射器很远时，接收器会变得越来越难接收信号。

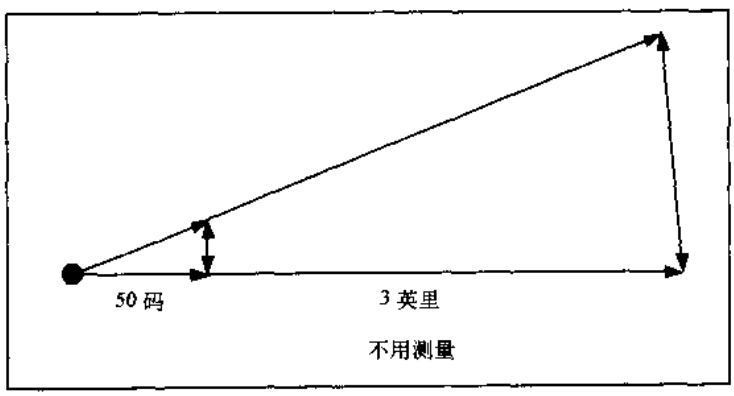

图 11-4　天线所对准的方向的一个小小的改变可能会对几英里外的接收器产生巨大的影响

用肉眼在山坡上的很多建筑物中寻找其中的一座，或者在几英里之外的河谷中寻找其他的端点也是很困难的，所以一副望远镜或者双筒望远镜就成了您的安装工具包中的必备品。从网络连接已经存在的地方的屋顶或顶层的窗口中开始寻找目标位置，如果能找到它，您就有可能在本地和目标位置之间安装一个网络链接。

然而，长的链路中至少有一个天线必须高到能够克服菲涅耳圈干扰和地球表面曲率所产生的障碍。对于一英里或两英里的链接，这不是一个严重的问题——屋顶或两层楼的建筑物就可能高到足够选择一条无障碍的路线，除非这条路线上有很多树——但是如果您准备将信号送到 5 英里或更远的地方，天线的高度就是一个重大的问题。这就是您经常看到广播发射塔都建在山顶和高楼的原因。

11.3.3　调整天线

为了获得最好的性能，定向天线必须直接对准链路另一端的天线。如果两端的天线都是定向的，则它们都必须正确地指向对方。大多数情况下，放置天线的最好位置是在屋顶或高塔上，或者用螺丝固定在外墙上，但是如果到链路另一端有一条无障碍的视觉路线的话，将天线放在屋内靠近窗户的地方有时候也是可以的。很多商业性天线都带有关于辐射(方向)图的资料——在水平方向和垂直方向上何处信号最强。如果有疑问，务必参考这个文档，因为所有的天线都不能立刻清楚最强的信号点在哪里。例如 yagi 类型的天线，在稍微偏离中心的位置上信号最强，在长距离的链路上这一点可能会导致您的安装成功或失败。

通过观察 Wi-Fi 配置软件中的信号强度显示功能来调整一对天线是完全可能的，但是当您操作长距离链路和弱信号时，一种称作频谱分析仪的测试设备会提供更多精确的信息。频谱分析仪是一种很贵的无线电接收机，它可以将无线电波频谱的一部分显示成可视图像。频谱仪用尖峰状图形来显示检测到的任何无线电信号，并且当信号强度增加时，尖峰状图形也会变大。这样您就能使用显示结果来给天线找到最佳可能位置。

不幸的是，能显示 2.4GHz 信号的频谱分析仪是相当昂贵的设备——一个新的频谱析仪可能价值几千美元。您最好是在需要用它安装天线的那天租或者借一到两台。如果不能轻易地找到频谱分析仪，也不要担心，Wi-Fi 软件中的信号强度显示也工作得较好。

给一个点到点链接安装和调整天线不是一个人能做的工作。最低限度也需要两个人，一个人调整天线的位置，另一个人观察计算机或频谱分析仪并找出最强信号。如果您能在链路的每一端都派一个工作组，并用电话或双向无线电通信设备联系的话，您将会节约很多时间，避免很多失误。

要正确对准天线，请遵照以下步骤：

(1) 选择您想安装每个天线的确切位置，并且将用来固定天线的杆子或柱子稳固地安装好。

(2) 使用每个天线附带的安装部件将天线安装到杆子、柱子或其他支撑结构上。让天线指向链路的另一端，但不要拧紧螺丝；因为您还需要更精确地调整天线的位置。

(3) 用馈电电缆将天线连接到无线路由器、接入点或网络适配器。如果您有可以工作在 2.4GHz 的频谱分析仪，将它连接到从天线引出的馈电电缆上。

(4) 把路由器或接入点连接到各自的网络上，打开两端的无线电设备。如果您正在使用频谱分析仪，将它调到接入点或路由器正在使用的无线电频道的频率上。如果没有频谱分析仪，就启动网络设备的配置工具。如果只有网络链接的一端使用定向天线，那么只需调整这一个即可。

(5) 慢慢地移动连接到路由器或频谱分析仪的天线，您应该可以看到当天线对准了链路另一端时出现的信号强度显示的峰值图形。先将天线左右移动，然后再调整垂直角度。当信号强度显示或频谱仪显示的是最强的信号时，拧紧天线的安装部件，保持这个位置。

(6) 如果另一个天线也是定向的，重复上面的搜索信号峰值过程。如果在远程位置有另一个工作组，他们就可一边使用电话或无线电通信设备和原始位置点的人通话，一边调整他们的天线。

(7) 如果天线还没有连接到网络设备，将天线引出的反馈线连到路由器、接入点或网络适配器。当整个过程进行到这儿的时候，您应该能够在两个端点之间双向交换数据了。

此时，应该可以在两个端点双向交换数据。如果不能通过链路获得足够的信号来生成可用的网络连接的话，您可能必须增加射频放大器来增强信号或将其中一个或两个天线换成具有更高增益的其他天线。

11.3.4 障碍物和中继

点到点链接中的每个天线都必须有一条无障碍的视觉路线通到链路另一端的天线。如果在源和目的位置之间有建筑物或高山的话，您将必须找一条通路，让信号穿过去或绕过去。如果信号路径穿过树木茂盛的地区，您应该在春季或夏季进行勘测工作，因为能毫无问题地穿过光秃树枝的信号常常会因为树叶或其他叶子而被切断。对叶子的安全的估计是每棵树损失 3dB，也就是信号功率损失一半。

您不能让无线电信号弯曲，从而绕过障碍物，所以通过障碍物的惟一方法就是在某一位置使用中继器，以使得到两个端点都有一条视觉路线。中继器可以是能够容纳两个无线收发设备的单个路由器，例如 Orinoco 室外路由器，也可以是两个通过以太网电缆连接的单独的路由器或者通过网络集线器连接的一对接入点。为了减小两个天线之间干扰的影响，多段网络链接的每段应该使用不同的无线电频道。

顺带的好处是，将网络中继到另一个无线设备处的路由器也可以给中继器所在地的建筑物提供网络服务，或者分割网络，将信号中继到两个或更多个远程端点。例如，Wi-Fi 网络的中央控制点可以放在河谷的谷底，并使用链路将其连接到附近的山顶和屋顶上的中继点。从山顶上的中继器出发，一个网络可沿不同的方向延伸到两个或多个位置。

11.4　802.11b 的替代品

长距离的 802.11b 链接不是将远程客户端连接到局域网的惟一方法。扩展网络的其他方法常常更容易或更可靠。

点到点无线链接使用 Wi-Fi 设备的主要原因是设备容易获得，相对便宜，并且不需要特别许可证，另外链路可以是已经存在的局域网的一部分。但是其他采用不同(得到许可或没有得到许可)的无线频率或不同类型无线电信号的收发设备也是可以使用的。

IEEE 802.11 规范(不包括 b)包括了使用直接序列扩频(DSSS)和跳频扩频(FHSS)的无线电波。在其他无线局域网产生的干扰成为问题的无线电环境下，不同的技术常常能降低噪声，产生强的、干净的数据流。

每种无线电类型都有不同的数据传输速率和信号范围组合。例如，Alvarion(以前的 BreezeCom)PRO.11 无线网络产品系列使用 FHSS 无线电波，能在 30 英里的距离上达到 3Mbps 的数据速率。BreezeNET 工作组网桥直接连接到 10Base-T 以太网。

如果 802.11b 的 11Mbps 数据速率不足以满足您的要求，其他设备能提供更快的连接，但是它们通常比 Wi-Fi 链接的距离更短。802.11a 设备的最大数据速率在 5GHz 时大约是 54Mbps。C-SPEC 的 OverLan HS 100 最高速率大约为 100Mbps。但是信号范围比 802.11b 链接小了很多。

Barry McLarnon 收集了一系列使用几个不同工作频率的无线局域网产品的信息，包括 915MHz、2.4GHz 和 5.8GHz，在 http://hydra.carleton.ca/info/wlan.html 处的 Web 站点是设备评论、文章以及厂商站点链接的极好来源。

这是一本关于无线网络的书，但记住练习的目的是网络连接而不是无线链接有时是有用的。如果远程位置已经存在宽带 Internet 连接，就应该继续使用它，因为点到点无线链接只是一种可能，并不总是最好方法。

例如虚拟专用网(VPN)能提供点到点无线链接的所有优点，并且没有安装一对天线的麻烦。就使用网络的人来说，使用 VPN 通道连接两个或更多个建筑物的单一网络看起来就像使用无线链接的网络一样。另一个经常有效的方法是使用公用事业的地下通道在两栋建筑物之间布设电缆。

11.5　网络适配器的天线

如果使用点到点链接来连接远距离的单个网络客户端，您将需要能使用外部天线的网络适配器。有几个厂商(包括 Zoom 和 Orinoco)供应带天线连接器的 PC 卡形式的无线网络适配器。ZoonAir 4103 型的网络适配器带有一个可拆卸的全向天线，如图 11-5 所

示，您可以用电缆和定向天线来替换。

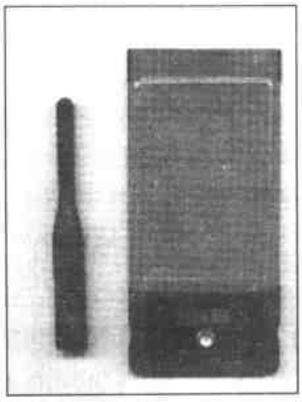

图 11-5　ZoomAir 4103 型适配器使用外部天线

Orinoco 的 PCMCIA 适配器包括两个内部天线和一个外部天线的连接器。天线连接器的位置在卡边缘上的小盖子下，如图 11-6 所示。您可以用针尖移掉盖子。

图 11-6　Orinoco 适配器上的天线连接器在 PC 卡的外端

因为 Orinoco 的适配器使用专有连接器，它需要一个称为“猪尾巴”的特殊电缆，在其一端使用标准天线的电缆连接器，另一端使用和 Orinoco 连接器匹配的插头。Orinoco 品牌的“猪尾巴”的价值可能超过网络适配卡，但是其他可以同样工作的猪尾巴也能够从另外几个厂商处得到(价格不及 Orinoco 的 1/3)，包括 Fleeman Anderson & Bord(http://www.fab-corp.com)，HyperLink 技术公司(http://www.hyperlinktech.com)和 Invictus 网络(http://www.invictusnetworks.com)。

11.6　制作您自己的天线

很多社区网络狂热者用奇怪的部件、塑料隔离物、铜线、空的锡杯和土豆片金属罐

等设计制造出他们自己的天线。用您的食品室或废料箱里的东西来做天线的话，一个自制的高增益定向天线的材料费可能只需要 3 到 4 美元，还不到一罐咖啡，牛肉炖菜，或土豆片的价格。如果您必须出去买所有的部件和工具的话，您可能必须得花 20 美元或更多。

不过，当您把装配天线及扭动天线以达到最佳性能的时间的价值都加进去的话，使用自己的天线是否比买一个不贵的商业性天线更便宜就不得而知了。花费 3 到 6 个小时或者更长时间安装一个家庭制作的天线并不是什么不寻常的事情。在线搜索几分钟(搜索“2.4GHz 天线”)应该可以找到几个出售 50 美元以下的定向天线的地方。它们至少都比您自己做的性能好。记住您的接入点或网络客户端适配器仅仅传输几分之一瓦特的功率，所以并不需要能够处理很高功率的天线；您可以用相对轻便的。

点到点通信中最常用的定向天线称作“yagi”或者更正确地称作 Yagi-Uda 天线系统。这是为纪念两个日本工程师而命名的。他们是 Tohuku 大学的 Hidetsugu Yagi 教授和 Shintaro Uda 教授。大约在 1926 年由他们设计并制造了第一个天线。典型的 yagi 天线(如图 11-7 所示)有一个惟一的有源元件，长度正好是工作频率的无线电信号波长的一半(在 2.4GHz 时约为 2.35 英寸)。四分之一波长的元件也能工作。被称作反射器和引向器的额外元件和有源元件平行放置。它们之间的特定间隔由有源元件的尺寸决定。反射器放在有源元件的后面，引向器放在前面。在有线电视和卫星电视出现以前大部分普通的屋顶电视天线都是 yagis 天线。

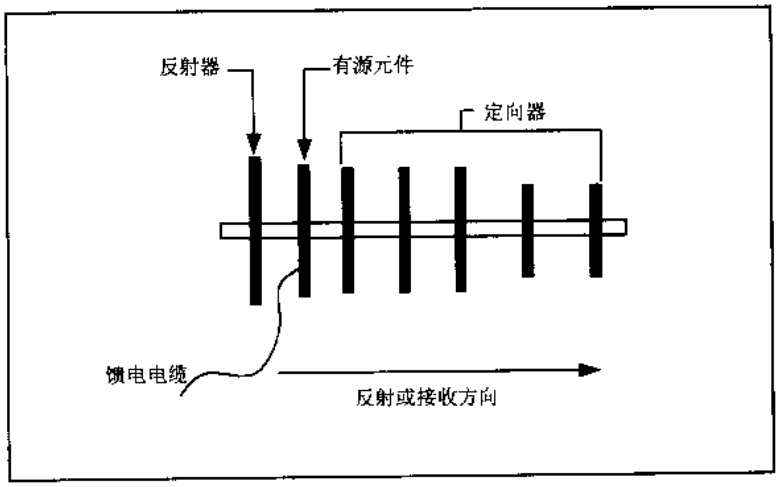

图 11-7　yagi 天线有一个有源元件，一个反射器和几个引向器

yagi 天线总是只有一个反射器和几个引向器，反射器比有源元件大约长 5%，定向器比有源元件短大约 5%(每一个引向器都应比它后面的引向器稍短)。yagi 天线的增益随着元件的增加而增大。如果您考虑做一个自己的 yagi 天线，可以到 http://www.oreillynet.com/cs/weblog/view/wlg/448 处看一看 Pringles 土豆片罐子里的

Rob Flickenger 天线。

很多 2.4GHz 的家庭制作的 yagi 天线使用一英寸的垫圈作为反射器、定向器和有源元件。它们可以工作，但是它们并不理想，原因有两个：第一，在 2.437GHz(频道 6 的中心频率)，四分之一波长有源元件应该是 1.16 英寸长，所以那些垫圈大约比理想性能所要求的尺寸小 16%；第二，反射器和引向器与有源元件一样大小，这会减小天线的增益(敏感度)。但是考虑到整个天线由价值约 7 美元的部件制作而成。这已经足够接近了。如果一对这样的天线能够以很高的速率来回发送信号的话，反射器和引向器的尺寸是不是恰好合适也就不重要了。

Darren Fulton 更为传统的 13 个元件的设计在 http://www.users.bigpond.com/Darren.fulton/yagi/13_element_yagi_antenna_for_2.htm 处，如图 11-8 所示。它使用大尺寸的黄铜或铜线制作的长度合适的天线元件和大片铝制成的反射器。

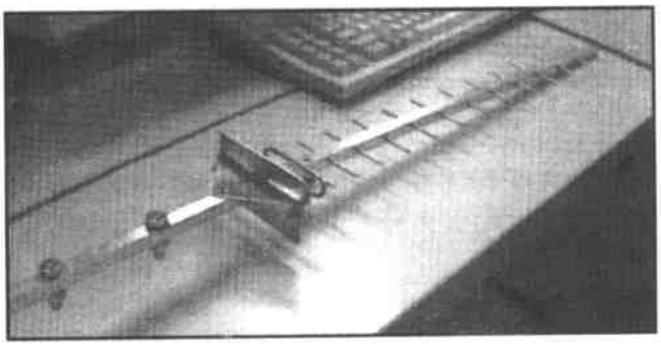

图 11-8　Darren Fulton 家庭制作的 yagi 天线有 13 个元件

yagi 不是可以自己制作的定向天线的惟一类型。在圆柱形或圆锥形金属反射物中放有辐射元件的波导天线使用另一种极有效的设计。天线的性能取决于外壳的尺寸、辐射元件的长度和它的确切位置。Greg Rehm 关于组装一个铁罐头波导天线的说明可从 http://www.turnpoint.net/wireless/cantennahowto.html 在线找到。

如果您想在所有方向上都增强信号，您可能想使用全向天线。Tim kyle 在 http://kyleti.aswwc.net/index.php?page=projects&old_project=80211b_Discone 处的 discone 设计看来是一个不错的出发点。

Internet 上供这些家庭制造的天线测试和测量的工具使得它们似乎既有效又便宜，尤其当您计算价格时不包括时间价值的情况下更是如此。这纯粹是一个态度问题：如果当您阅读制作家庭制造天线的资料时认为“那听起来似乎是有趣的计划”，那您就去做吧。但是如果一个下午手上都拿着烙铁听起来是一种痛苦和不寻常的处罚的话，请记住一个便宜的商品天线可以将同样的工作做得很好，并且要省事得多。

第12章　公共网络和社区网络

提供无线网络接入给商业公司和家庭的 Wi-Fi 网络技术同样也允许用户从包括旅馆、会议中心、机场客运枢纽站的其他位置将他们的手提计算机和掌上设备连接到 Internet。很多 Internet 服务提供商，蜂窝电话公司和独立的无线网络服务商已经建立了公共的 Internet 热点。不断增长的咖啡店、餐馆和类似商业公司是这些热点的主人，并寄希望于它们会鼓励顾客在阅读电子邮件和浏览 Internet 时将时间和金钱花在他们的设施上。

在工作时和在家里使用无线网络的人们可以用同样的手提计算机和网络适配器收发邮件，浏览 Internet 以及通过公共无线服务交换文件。这些服务提供每次付费式的用户接入和月租式的用户接入。在可以接入的情况下，这些网络能够提供方便快速的 Internet 和企业网接入，作为拨号连接的相对便宜的替代品。

无线网络技术也催生了新一代业余爱好者和社区组织者，他们在屋顶或山坡上安装天线，使得公共无线网络可以覆盖整个附近的区域。

到现在为止，我们已经分别讨论过建立和操作您自己的无线网络，并将计算机连接到该网络。本章将阐明在何处和如何找到公共网络以及如何配置您的计算机来使用它们的服务。

私有无线网和公共无线网的最重要的区别是网络的拥有者和管理者加在他们用户上的访问控制的数量和类型。位于办公室，工厂或大学校园的私有网可能使用一些密码组合，WEP 加密以及保密的 SSID 来防止非授权用户进入。与之相对，大部分公共网络配置成“信息实用工具”，对任何有网络适配器和信用卡的人都是开放的和可接入的。

在无线接入成为现实之前，很多人在他们离开家或办公室的时候需要使用 Internet 或连接到他们的企业网的话，就使用拨号调制解调器和电话线来建立连接。这样是可以的，但是找到一个有合适插头的公共电话，将计算机平稳地放在电话亭的小架子上，以及找到一个能接入到您的 Internet 服务提供商，而且不是所有时间都是忙音的本地电话号码常常是非常令人讨厌的事。如果您幸运的话，您可能会获得实在的 56Kb/s 的连接。无线接入到 Internet 相对于拨号方式有几个典型的重要优点：它是快速的，它能立刻提供连接，它使用代替电缆的无线信号，所以您不必连到附近的电话插座上。

通过蜂窝电话连接如何呢？可以连接，但是在您开始使用网络之前，通常需要一系列冗长耗时的拨号过程，包括登记、连接、校验等。当您确定连接上之后，链接又是很慢且容易中途掉线。其他无线服务例如 CDPD(蜂窝数字分组数据)比蜂窝电话和调制

解调器更容易更可靠，但是最大速率是相对较慢的 19.2Kb/s。Wi-Fi 连接几乎是立刻的，并且数据速率也是很快的。

大多数连接到公共无线网络的人使用它们连接到 Internet 或者他们老板的企业网。与私有无线局域网的用户不一样，人们通常不使用公共网络和同一局域网内的其他计算机共享文件或发送文档到本地打印机。而特别的对等网络和红外链接是实现那种直接文件传输的更好方法。

12.1 公共网络

公共网络根据接入无线 Internet 的分钟数或天数来收费，并且也提供不限制连接时间的每月收费一次的方式。大部分公共网络常常放在商务人员最可能需要快速方便的电子邮件和 Internet 服务的地方以及餐馆和咖啡店里，因为它们的主人希望顾客在浏览网站和阅读邮件时能多买一些咖啡和糕饼。少数的公共无线网络甚至放在投币洗衣店里。

由于无线服务已经引入到旅馆和会议中心，用太多的 PowerPoint 幻灯片举办那些冗长会议的人们开始注意到，他们的一些听众正在将更多的注意力放在他们面前打开的笔记本电脑上了，而不是房间前面的演讲者身上。他们可能是用半只耳朵在听下一年度的市场计划，不过有些人正在全神贯注于他们的计算机从空中接收到消息或网页，另一些人在将他们关于演讲的笔记和注解发送到 Web 日志上或传给没有参加会议的朋友和同事。这是否会迫使演讲者将他们的演讲变得更有趣？不要屏住呼吸。但这可能会使得听众使用即时消息来不断地对演讲者进行评论成为可能(只是让他们不要在错误的时间笑)。

公共无线网络行业仍然处于早期。在北美及欧洲的少数的机构和旅馆以及两百个左右的咖啡店里已有了无线信号，但是那只是未来几年里公共无线网络可能覆盖位置的极小一部分，尤其当内置无线适配器成为新的笔记本电脑的标准配置的时候。

现在，还必须拥有多个公共和社区无线服务的帐号，从而达到真正大范围的覆盖。比如说，如果您把您的笔记本电脑或 PDA 从 Boingo 服务的机场带到有 hereUare 热点的咖啡店，您将同时需要这两个服务的帐号。随着无线 Internet 服务提供商(WISP)行业的发展和成熟，在不只一个无线 Internet 服务提供商(WISP)的热点区之间漫游将会变成平常的事情，并且允许用户使用一个帐号从多个位置连接到 Internet。WISP 公司正在制定漫游计划，以允许用户使用他们的帐号在附近的公共接入点之间漫游。即使属于不同的服务提供商也无所谓。

最终，无线网络服务应该会像蜂窝电话一样实现无缝地覆盖：您只需要打开计算机并且在公共接入点的范围之内，您就能登录到网络。只不过我们现在还没有达到这种水平。

12.2　建立到公共网络的连接

就像与无线以太网相关的任何事情一样，接入到公共网络几乎总是需要一些无聊的计算机网络配置。如果您读过(甚至只要浏览过)本书前几章，您就可能比百分之九十的使用无线网络的人知道更多关于无线网络配置的知识，因而为 WayPort 或其他某个公共网络添加新的设置应该不是难事。

12.2.1　查找网络

有两种方法可以找到公共无线网络：您可以参考印刷出版的(或在线的)目录，或打开计算机查看在某一范围内是否有网络。如果您的无线网络配置工具不能自动显示它检测到的所有网络信号的 SSID，您最好在尝试连接之前查询一下每个服务提供商的目录。但是如果您正使用一个系统，它可以扫描附近信号并让您选择使用其中一个的话，您可能会发现任何目录都没有列出的公共无线网络。

然而，这是一种牌子的无线网络适配器和另一种不一致的特征之一。可能的情况是您的配置工具会显示一个它检测到的网络列表，并且让您选择一个加入。如果您正使用苹果公司的带有 AirPort 卡和 AirPort 软件的 PowerBook，软件会在 Control strip 模块和 AirPort 应用程序显示附近无线网络的菜单。Windows XP 的无线网络设置工具也可以做同样的事情；在某些 Windows 和 Linux 工具中，当 SSID 没有定义或被设置成“ANY”时，适配器会自动将自己关联到检测到的第一个网络。如果您的适配器被设置成检测未知网络的话，无论何时，只要有一个公共网络在范围之内，它都应该能找到。

当然，在搜索过程中，您会发现很多网络是私有局域网而不是公共网络。这些网络中有一些外部用户能够接入，因为网络的所有者可能没有成功地应用 WEP 加密和 802.11b 标准的其他安全特征；但是偷取服务和利用公共网络确实是有区别的。

加入一个已知网络比寻找随机信号几乎总是容易些。当您在某个公共网络服务中建立了自己的帐号时，您就可以建立一个可供选择的配置资源文件用来检测那个网络。有些配置工具能自动扫描他们的资源文件的列表，而其他一些需要用户手工改变资源文件。不管是那种方法，当您的手提计算机在该服务的范围之内时，它就可立即将自己联入您想要加入的网络中。

每一个活动的公共网络服务在它的 Web 站点上都有“哪里可以找到我们”的页面，上面列出了它所有的活动位置。所以当您到达 Boingo 服务的机场或 T-Mobile 网络覆盖的咖啡店，您就可以激活该服务的配置资源文件，无需搜索服务，直接登录即可。此外，有几个网站提供包括多个服务提供商经营的接入点和热点的联合目录。包括 http://www.wifinder.com 和 http://www.80211hotspots.com。

如果您不知道哪一个公共无线服务与您正等着更换航班的机场或您正参加会议的会议中心有网络服务合同的话，将不得不让您的计算机搜索信号。如果您还没有那个无线服务提供商的帐号的话，不要着急；很多 Internet 服务提供商都允许新用户现场创建新帐号。如果您够幸运，这个服务提供商可能与您已经登记的服务有漫游协议，这样您就不用去建立新帐号了。

从商业公司之外的管理接入点的地方登录到公共网络常常是可能的。例如，Tully 的咖啡店是基于西雅图的咖啡连锁店，它的不动产策略是在已经存在的 Starbucks 批发商店附近开办它们自己的商店。它还没有提供 Wi-Fi 接入(计划将来提供)，但是它的很多顾客通过附近的 Starbucks 的接入点登录进去。Tully 的董事长 Tom O'keefe 告诉《西雅图时代》，“一切就这样发生了，他们在我们的商店里，喝着美妙的 Tully 的咖啡，品尝着我们的硬面包圈——步入街对面的 Starbucks 的 Wi-Fi。您知道的，Wi-Fi 会旅行。”

查找无线网络信号的特定步骤对于不同的操作系统和配置工具是不同的，但是基本步骤总是一样的。在改变您的计算机的网络设置和连接资源文件之前，在笔记本或其他您能找到的地方保存一个初始设置的备份。当您返回到您自己的办公室或家里的网络时，您可能需要返回到以前的设置。

搜索无线网络遵循以下步骤：

(1) 如果还没有连接，将无线网络适配卡插入到您的计算机的 PCMCIA 插槽或连接到计算机的 USB 端口上。

(2) 如果还没有开的话，就打开计算机。

(3) 使用计算机的 TCP/IP 网络设置工具，命令计算机从 DHCP 服务器处获得一个 IP 地址。

(4) 将改动保存在网络设置中，如果有必要重新启动计算机。

(5) 打开网络配置工具。

(6) 如果您知道您想使用的网络服务的名称，在活动连接配置文件里将该名称设为 SSID。如果您想搜索网络，将 SSID 设为“ANY”或者让 SSID 保持为空。

(7) 选择新的资源配置文件作为您的活动资源文件。

(8) 打开无线状态工具。

如果您的计算机在无线网络范围之内，状态工具将会显示信号的强度和质量，也可能会显示网络的名称，这取决于程序。

1. 在 Windows XP 中搜索网络

在 Windows XP 中，搜索网络甚至更容易：

(1) 将您的无线适配器插入到计算机的 PCMCIA 插槽或将它连接到 USB 端口。

(2) 如果计算机没有开，则打开计算机。

(3) 双击系统面板(在时间附近)中的 Network 图标。如果无线网络适配器检测到附近的一个或多个信号，将打开 Wireless Network Connection 状态窗口，如图 12-1 所示。

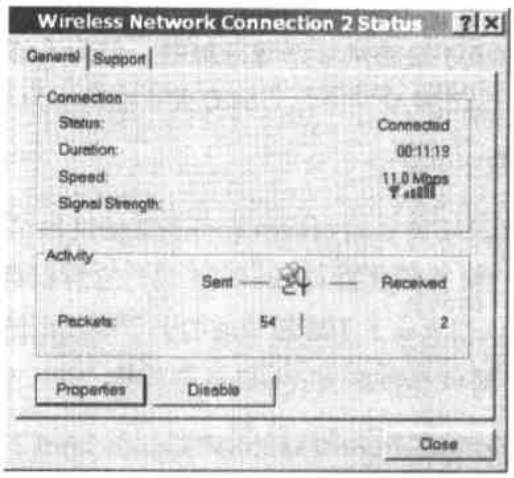

图 12-1　Wireless Network Connection Status 窗口显示无线链接的状况

(4) 单击 Properties 按钮，单击 Wireless Networks 标签。打开如图 12-2 所示的 Wireless Connection Properties 窗口。

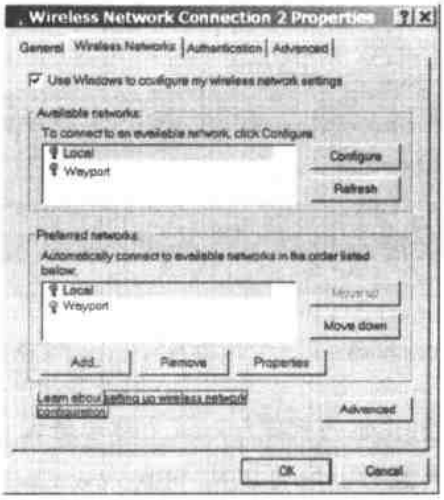

图 12-2　Wireless Connection Properties 窗口显示本地计算机范围内无线网络列表

(5) 可获得的网络列表显示无线适配器检测到的所有活动网络。要连接到其中的某个网络，从列表中选择网络的名字，单击 Configure 按钮。

(6) Windows 自动填充 Network Name 栏。公共网络通常不使用 WEP 加密，所以可忽略 Wireless Network Key 部分。单击 Cancel 关闭窗口。

(7) 单击 Properties 窗口的 OK 按钮，然后单击 Status 窗口的 Close 按钮。

一旦找到一个网络并建立连接后，就可以打开 Web 浏览器。如果浏览器设置成自动打开主页，它将不会去找那个页面，而是去打开公共网络服务的登录页面。如果您还没有这项服务的帐号，按照屏幕上的提示创建一个新帐号。如果您的浏览器设置成启动时打开空白页面，它就不会自动显示登录屏幕，但是当您试着从您的书签或收藏夹列表中(或其他 Web 站点)连接到某个站点时登录页面将会出现。

2. 无线网络搜索工具

如果您的无线配置工具不能自动扫描所有可获取的网络信号的话，Marius Milner 的 Network Stumbler 是一个很巧妙的 windows 工具。它可以帮您找到它们并显示一个如图 12-3 所示的列表。该列表显示了您想知道的关于检测到的网络信号的任何信息，包括 MAC 地址、SSID、通道号码以及信号强度和质量。

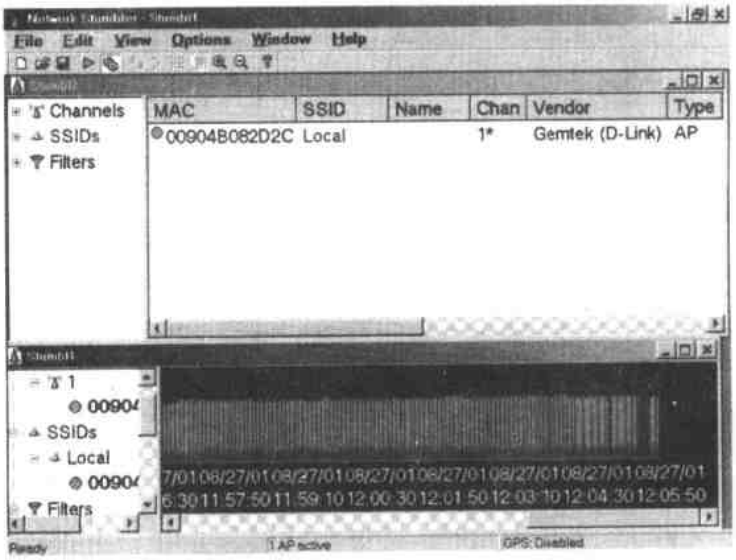

图 12-3　Network Stumbler 找到并显示它能找到的每个无线以太网信号的大部分细节

Network Stumbler 是一种“乞丐软件”，这个意思是说它可以免费获得，但是鼓励认为它有用的用户捐款给开发者。您可以从 http://www.netstumbler.com/download.php 处下载 Network Stumbler。

无线热点的主要经营者 Boingo Wireless 提供了它自己的免费搜索程序。如图 12-4 所示。Boingo 的软件以它自己的站点为特色，但是也可以检测和显示其他公司经营的热点。从 http://www.boingo.com 处可下载 Boingo 软件。

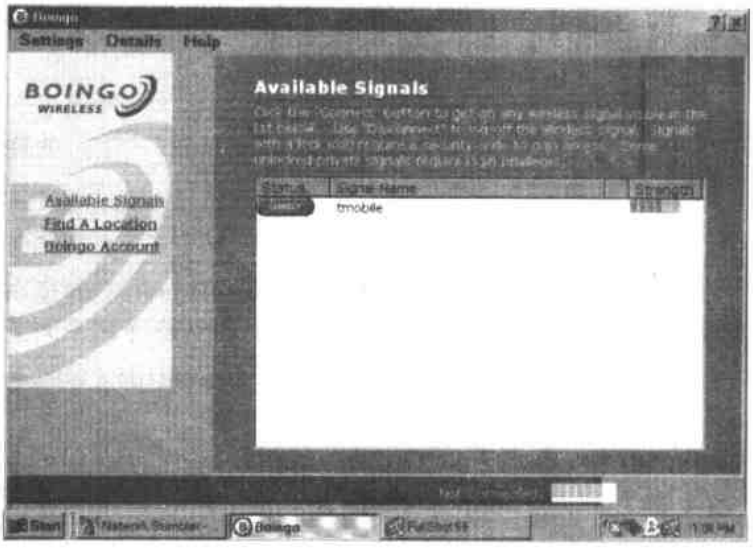

图 12-4　Boingo 软件在您的 Wi-Fi 适配器范围内可识别活动的无线热点

Hewlett-packard 的无线连接管理器是另一个可以检测和连接到 Wi-Fi 网络的免费程序。遗憾的是，它仅在 Windows2000 或微软 Pocket 2002 以及康柏的 WL110 无线 PC 卡上运行，所以对大多数用户没有用处。但它是免费的，所以如果您恰好有合适的硬件和软件的话值得一试。需要获取更多信息，可以到惠普网站 http://www.hp.com/solutions1/corporatebusiness/wcm 上查看。

Wardriving.com(http://www.wardriving.com/code.php)网站的软件页面有很多搜索 Wi-Fi 信号和提供附加的安全和控制的其他工具的链接。

12.2.2　通过公共网络发送邮件

很多商业性的局域网和 Internet 服务提供商都将他们的邮件服务器配置成让用户可以从 Internet 任何地方接收邮件。但是发送邮件时只接收网内的邮件。这个限制阻止了垃圾邮件传播者和其他未授权用户通过未受保护的服务器中转信件，但同时也使得合法用户在离开家时发送消息变得困难。

为了克服这个问题，很多公共 Internet 服务的邮件服务器接收临时登录到网络的用户的外发邮件。如果您常用的服务器在您从公共无线网络连接时拒绝您的消息，可以试试更改您的邮件客户端程序的 SMTP 服务器名称。SMTP 服务器的名称是通常是 mail.[网络名]。如果这还不能正常工作，就去询问公共网络的技术支持中心。当您回到家里时，别忘了将设置改回到原来的服务器。

12.2.3 机场的公共网络

在机场候机厅提供公共无线网络服务是一种新兴的产业。从用户的观点来看这似乎是简单的——只需安装足够的接入点来覆盖所有的机场大厅和航空公司的休息室，然后将它们连接到宽带 Internet 干线上。接下来就是等着顾客付钱接入网络。这听起来就像是得到了印钞票的许可证。当然这并非那样简单。既然 .com 的投资泡沫已经破裂，新的 Internet 服务就更难盈利。从政府拥有的机场管理局到支持许多不同无线服务的设备都是不简单的，这些无线服务用来管理从空中交通管制到租用汽车的返回以及区间公共汽车的任何事情。

协调好所有这些无线电波并不是一件简单的事情。主要机场的技术设备经理坚持对在他们的物业范围之内工作的每个无线电发送机都实行完全控制。必须确保出租车调度员在客运枢纽站前面的无线电通讯设备不会与消防车或舷梯上的对讲机互相干扰。控制塔里的飞航管制员必须与地面和空中的飞机对话。一打或更多的航空公司都需要有他们私有的公司频道，四五个单独的蜂窝电话公司和寻呼服务公司都希望在每个机场大厅添加发送机来给他们的客户提供服务。还有不要忘记提供信号给那些在每个门口播放 CNN 节目的电视机的架在屋顶的卫星电视天线，或正在向在车库里寻找位置的人们广播的低功率的调幅广播电台。增加未经授权的无线以太网服务对机场无线电专家来说实在是又添了烦恼。

当机场和某个无线服务商签订特许权协议，当航空公司和另一个不同的公司签订合同以便给它们的 VIP 俱乐部提供无线服务时，问题变得更复杂了——机场会允许航空公司在租用的地方提供无线服务？或者机场范围的交易优先？两种服务是否会互相干扰？它们是否会和其他的无线服务发生干扰？谁来控制发射器？

每个机场的管理对这个问题都有着不同的回答。所以您不能指望为连接到芝加哥的 Admiral 的俱乐部而建立的帐号在西雅图靠近 A-14 门的等候区会有效。为了找到网络，您惟一能做的事情就是打开计算机，将 SSID 设成“ANY”，查看是否检测到信号。如果无线网络功能告诉您它找到了一个信号，记住去看一下显示本地范围之内所有网络名称的菜单或窗口。如果您有这些网络中某个网络的帐号，就可以继续下去，登录到网络。如果没有，选择一个信号最强的网络，新建一个帐号。

如果您旅行时经常经过同一个机场，或者您属于某一航空公司的 VIP 俱乐部，您可能想创建一个在这些位置提供服务的公司的预付费帐号。当您发现您在某个使用不同服务的机场(或其他位置)时，您通常可以现场注册离开时付费的帐号。

目前，下载并打印每个您拥有其帐号的公共无线服务当前的“哪里可以找到我们”的列表，并将它放在装计算机的包里几乎是很关键的。某些服务在某些机场并没有覆盖所有客运枢纽站的接入点，但是它们可能覆盖了一个有限的区域。比如个别航空公

司的大厅或名牌咖啡店。举例来说，如果您已经支付了 Boingo 的无限制的服务，您可能想使用它的服务，即使这可能意味着将计算机拿到机场别的地方。

当不同的无线服务签订了它们的漫游协定后，整个过程将会变得更容易。您将会拥有一个您最常使用的服务的帐号。无论您旅游到哪里，您都可以使用预付费的连接时间。无线网络会关心您的漫游服务的帐单，所以您不必担心。但是在那些协议还没有生效之前，您每次登录到新的服务时还是需要一个不同的帐号。

1. T_Mobile 热点

蜂窝电话公司 T-Mobile 管理着美国最大的无线网络服务提供商之一。用以扩大网络覆盖面积的覆盖区域覆盖了包括机场、航空公司俱乐部、旅馆、饭店和会议中心的商业带。它的网络在很多美国的航空终点站和 Admirals 俱乐部都是可接入的。T-Mobile 还有一个合作交易，以便 2003 年底之前在超过 3000 个 Starbucks 咖啡店提供无线网络服务。Starbucks 董事长 Howard Schultz 预期“这将会给商店带来很多新顾客，并且很多人将会呆更长的时间。”

T-Mobile 提供一系列服务计划以满足临时用户、经常来的旅行者和计划在一个城市地区内使用网络的用户的不同需求。您可以在 http://www.t-mobile.com 处选择最适合您需要的计划。Starbucks 在它们的咖啡店提供 T-Mobile 热点服务的一天免费试用。在 http://www.starbucks.com/retail/wireless.asp 处查看 Starbucks 网站获取最新的升级代码。

2. Boingo

Boingo 是公共无线网络服务提供商两大巨头的另一个。Boingo 在航空终点站、旅馆、会议中心和其他为商务旅行者服务的位置都有无线网络。它的机场网络包括 Dallas-Fort Worth，Austin，西雅图和圣何塞，而且它还宣布了在亚特兰大，芝加哥、华盛顿、波士顿的机场引入额外附加服务的计划。Boingo 最近的活动站点目录在 http://www.boingo.com 处可以获得。

3. hereUare

hereUare 不是无线服务提供商，但是它提供的帐号允许用户连接到几个网络拥有和管理的无线热点。一个用户 ID 和密码可以在任何加入的位置使用。

遗憾的是，覆盖范围最广的几个无线网络都没有加入到 hereUare 的计划，不过很多其他的网络加入了。您可以从 http://www.hereuare.com 处下载它的全球探测软件，该软件提供可搜索的 hereUare 站点列表。

12.3 私有网络的公共接入

很多商业公司和社会事业机构，比如大学、医院和图书馆都经营他们自己的无线局域网，允许访问者通过他们的网络连接到 Internet。在可以获得这类服务的地方，网络经营者可能准备了说明书用来解释如何配置计算机使用该项服务。如果您正在访问某个可能有无线网络接入的公司，询问接待员或您要访问的人可获取更多信息。

12.4 加入社区网络

无线社区网使用 802.11b 网络技术在邻域范围内或整个城市共享高速 Internet 接入。这些网络的管理者在屋顶或其他可达到最大覆盖范围的位置为接入点架设天线。

除非您用高增益天线，无线以太网信号的最大有效范围只有大约 300 英尺(100 米)。不过，那可能已经足够提供服务到城市的半个街区了。而且如果更多的志愿者在他们的屋顶上安装额外的接入点的话，覆盖面积可能会更大。一些社区网络也使用定向天线建立点到点链接(经常使用由锡杯制作的反射器和其他低价部件，如第 11 章所述)来将网络的覆盖区域扩展到本地接入点范围之外的地方。

最后，这些网络的组织者希望建立无缝的“可选网络”，来提供免费的或价格很低的 Internet 接入给整个周围地区或整个城市和都市区。如果他们成功的话，应该可能在网络覆盖区域之内的任何地方都可找到免费的或便宜的无线 Internet 连接。如今，活动站点的数量仍然很少，所以您是否在网络信号的范围之内纯粹要看您的运气了。

这仍然是一个主要由激情的技术怪人和网络黑客组成的基础性的运动。但是它却有潜力对价值几十亿美元的被认为是下一代移动连接的 3G(第三代蜂窝移动通信)无线网络的形成有力的竞争。如果一个或多个用管子套着的带子和 Pringle 土豆片罐匆匆拼凑起来的非商业性网络，能以接近 11 Mb/s 的速率提供周围地区甚至整个城市的完整覆盖的话，3G 蜂窝网的支持者们将很难说服人们去购买他们昂贵的 9600Kb/s 服务。商业性的蜂窝网和无线网络的运营商们正在密切关注着社区网络的动向。

社区无线网络通常是由志愿者推动的合作性的服务，它们管理公共网络来提供 Internet 接入给或大或小的地区。在某些城市，包括西雅图、旧金山和伦敦，本地社区网吸引了许多基站和中继点。在澳大利亚，公共无线电网络正在几个城市里运转，而另一个组织正在讨论将网络覆盖到岛屿之州，塔斯马尼亚州。

很多社区网络组织雄心勃勃地计划将服务延伸到更广区域，但是他们实际操作时经常只有少数接入点，这些接入点可能互相连在一起，也可能没有。在近期的发展阶段，社区网络更多是出于一种好奇，而不是一种有用的资源，因为他们还没有很大的覆盖

面积。今天，社区网络实际上不过是可能共享同一个 SSID 的少数几个独立热点的网络。如果有一天这种情况改变了，社区网络将会变成城市通讯基础设施的很重要的组成部分。

Personal Telco Project 在 http://www.personaltelco.net/index.cgi/WirelessCommunities 处维护到世界上各个活动网络的链接目录。在 Personal Telco Project 列表中的大多数网络都有在线地图和节点列表，显示他们的活动接入点的位置。例如，图 12-5 显示了 PDX 无线网络在俄勒冈州波特兰市市区和周围地区的接入点。

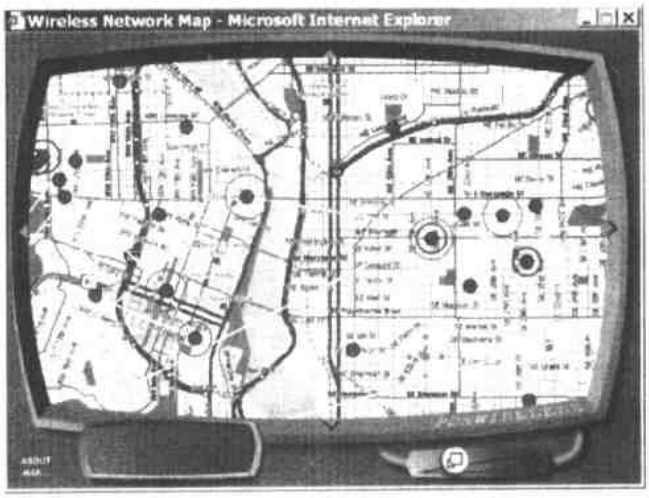

图 12-5　PDX 无线网络在波特兰市威拉米特河两岸都有接入点

社区网络是 802.11b 商业网络的有益补充还是它的重要竞争对手，这取决于您的观点。当 T-Moblie 公司在波特兰市 Pioneer Courthouse 广场的 Starbucks 商店安装一个无线热点时，它选择了社区网络已经使用的用来提供免费服务的工作频道。当然这样的安排对两个网络都产生了严重的干扰。经过了几天的争吵之后，T-Mobile 改用了另一个频道。

如果您找到了一个社区网络信号，它通常欢迎您使用它连接到 Internet。但是不要期望能从网络经营者那儿得到很多的技术支持或其他帮助。很多社区网络者都会乐意提供力所能及的帮助，但是这些网络是免费服务；不能像期望商业性网络服务提供者那样地要求它随时提供服务。如果您确实需要帮助，可以试试发一封礼貌的电子邮件到网络协调员那里。邮箱地址在网络目录中。

社区接入点的拥有者们都会对使用他们的网络做一些限制，不过这些限制通常都是那种很容易接受的常见规则：不要发送垃圾邮件，不要尝试传输极大的文件等。首要的基本规则应该是“不要做任何会干扰网络运转的事”。

如果您希望使用社区无线网络链接作为您永久的 Internet 连接，让接入点的拥有者知道您在哪儿是一个很好的主意。如果您离接入点足够近，可以整天使用接入点，那

么它的拥有者可能就是您的邻居。如果您什么时候带着一炉自制的小甜饼出现在他的门前时，他会非常惊喜的。社区网络通常由热心的志愿者组织管理；如果您利用了他们的成果，可以考虑加入到该组织，贡献自己的力量。即使您没有很好的技能，也总是可能找到其他方法来做出贡献。

在您可以使用社区网络之前，您必须找到一个信号并考虑清楚如何配置您的计算机的网络设置。使用与 Network Stumbler、Boingo 或 Windows XP 和 AirPort 里的无线配置工具一样的嗅探程序可能会找到多个信号，但是即使您找到了一个活动信号，您也不能区别它到底是欢迎您使用的社区网络还是没有很烦琐地开启网络安全功能的私有网络。最好使用每个社区网络分布在 Internet 上的在线指导。每个网络接入点的说明应该会向您提供建立连接所需要的信息：接入点的位置、网络的 SSID、DHCP 是否启动等。

12.5 公共网络的安全

网络安全朝两个方向发展——网络管理员不希望非授权用户搅乱网络，个人用户不希望任何其他人访问他们的个人文件。当您登录到一个公共网络时，您应该做一些预防措施以防止网络上其他人读取文件。您应该记得在您试着接到公共网络之前关掉文件共享。

在 Windows 95、Windows 98 和 Window ME 中使用以下步骤：

(1) 从 Control Panel 中打开 Network 对话框。

(2) 单击 File and Printer Sharing 按钮。

(3) 在 File and Printer Sharing 对话框里，禁用 I Want to Give Others Access to My Files 选项。

在 Windows 2000 和 Windows XP 中，没有集中地关闭文件共享的地方，您必须分别关掉每个共享。按照如下步骤关闭共享：

(1) 打开 My Computer 窗口。

(2) 所有共享的驱动器和文件夹的图标都以一只手托着图标的形式出现。要关闭共享，用右键单击图标，从弹出菜单中选择 Sharing and Security 子菜单。

(3) 关闭 Share This Folder on the Network 选项。

(4) 单击 OK 按钮关闭该对话框。

(5) 对每个共享文件夹或文件重复同样的过程。不要忘记共享文档文件夹。

当您回到您的办公室网络或家庭网络后，您必须进行相反的过程来重新共享您的文件。

通过无线链接传输数据时别人获取到数据的危险有多大呢？窃取数据是可以做到的，即使您使用 WEP 加密。但通常不太可能，除非您是政府调查或工业间谍的目标。

您必须假设任何通过无线网络传输的数据都是不安全的。一个执着的偷听者使用合适的设备和软件能够拷贝到空中传输的数据报。

能够绝对保证没有人正在监视您的无线网络的惟一方法就是停止使用它。在厨房里监听无绳电话甚至更容易。通常，您可以假设通过公共网络的连接不比到您自身网络的链接安全。如果有人一定要盗取您的网络上的数据包，他就可能找到一个方法做到。保护自己的最好方法是减少通过网络发送敏感数据的数量，并且当您必须发送私有信息时总是使用强大的加密方法，例如 SSH(加密的 Telnet)或 VPN(虚拟专用网，很多公司使用它来为外部用户提供到企业网的安全访问)。这一类的安全问题与公共网络没有直接的联系。关于网络安全的更多详细信息(或遗漏的部分)，请阅读第 14 章。

第13章　游击式联网

游击式联网(也称为 wardriving)是对从没有进行保护的无线网络窃取 Internet 接入行为的文雅的称呼。这可能是非法的，一定是不道德的，在很多地方无线网络的所有者或管理者没有使用 WEP 加密或其他方法来保护他们的网络，使得游击式联网特别容易。在很多市区办公区域、高技术工业园区和高档住宅区，一个偶然的访问者常常能在几个街区之内找到并登录半打甚至更多的无线网络。

如果您能检测到一个网络信号，您就可能登录或者通过该网络连接到 Internet。使用正确的软件工具，您就可以在其他用户的数据通过网络时监视它，并且破解它们的 WEP 密钥。当然，读这本书的人都不会考虑尝试登录到别人的网络，或者未经允许进行窃听，所以我不会探讨任何关于如何以及在何处建立连接的问题的细节。如果您想尝试，这是您自己的事。用一个好的 Web 搜索工具搜索几分钟，您就可以找到一个很多普通接入点使用的默认 SSID 和 WEP 密码列表以及用来破解 WEP 加密的软件。很多用户(尤其是家庭网络和小型商业网络的用户)没有打开 WEP 加密功能，因为它“太复杂”或“太麻烦”。还有很多用户根本就不改变默认设置。

说一个没有保护自己网络的人应该得到外人入侵的惩罚确实有点苛刻了。但是再强大的安全工具，如果您不使用它，也不会有任何作用。

这一类准法律的无线网络入侵或者说是 wardriving，是那些老黑客的 wardialing 行为的扩展——使用调制解调器随机地拨一个电话号码，搜索有未受保护的拨入端口的其他计算机。

如第 12 章所述，有些无线网络实际上是欢迎公众接入的，所以 wardriving(或者使用支持 Wi-Fi 的 PDA warwalking)也有合法的原因。即使您实际上并不想建立到某个网络的连接，在您的附近转转，看看周围都有哪些网络也是有益的(并且也是有趣的)。

13.1　公共网络的安全

作为您自己的无线网络的管理者，这将会在您的头脑中产生整个一系列的问题。比如像这样的问题：“我的网络安全吗？街上的某个人可以在没有我的允许的情况下接入到我的网络吗？我怎样才能将那些#*@&$!字符排除在我的网络之外呢？”要寻找这些问题以及其他关于无线网络安全问题的答案，可以直接转到本书的第 14 章。

最起码的，您应该知道 Wi-Fi 网络不是绝对安全的，每个 802.11b 接入点和网络适

配器发射出的信号都可能被外来者检测到。您可以逐步限制别人访问您的网络，但是对于认真的探听者来说，您的网络不可能始终是一个秘密。

13.2　嗅探工具

嗅探工具是一种程序，它使用无线网络适配器扫描活动的网络，并显示每个网络的特征。前面章节中描述过它们，它们对于找到不很明显的 Wi-Fi 信号也是很关键的。

Windows 中使用最广泛的嗅探工具是 Network Stumbler 的 Windows 版(http://www.netstumbler.com)；如果您正在使用 Linux，Kismet 是最常用的工具(http://www.kismetwireless.net)。但是它们不是惟一的选择。Windows XP 的无线配置和控制软件，几种牌子的网络适配器提供的程序(包括 Orinoco 和 HP-Compaq)，以及 Boingo 无线工具(从 http://www.boingo.com 处可获得)都提供类似信息。

使用这些工具中的任何一种的过程都是很相似的：打开您的安装有无线适配器的计算机，运行嗅探工具检测和显示附近的信号。用嗅探工具提供的信息配置适配器来创建一个连接。

13.3　搜索信号

如果您准备花费大量时间带着笔记本电脑驾驶着汽车在附近搜索网络的话(做这些靠步行是极不实际的，除非您在市中心)，您就可能想装配特殊的 wardriving 工具箱。它包括了最适合做这项工作的工具：一个可以使用外部天线的网络适配器(像 Orinoco 或 Zoom 公司的)，一根允许您从汽车打火器给笔记本电脑提供电源的电缆以及一个比适配器里的天线有着更高增益的天线。

如果您不能确切地知道附近的 Wi-Fi 信号从什么地方发出，您最好的选择就是在汽车顶上装一个全向天线。Orinoco、HyperLink 和其他厂商制造的 2.4GHz 移动天线可以很好地胜任这项工作。不过，如果您不想花钱进行永久性的安装，则可以临时配备一些东西：一个带引出线的适配器，一些带有夹子的导线，可能的话带上一个 2.4GHz 无绳电话上的天线，或者甚至是外衣的衣架或其他较硬的线。这些不是很好的东西，但是即便是便宜的、脏的临时性应急的东西也可以做这些事。很多针对全向天线的计划在 Internet 上都有，很快地搜索一下就可以迅速找到。

也可以试一试用锡杯或 Pringles 土豆片的罐子做的定向天线，但是定向天线不是用来寻找未知接入点的最好工具。您必须实实在在地移动天线指向您经过的每幢建筑物来搜索可能的信号。很明显，当您不想吸引很多注意力的时候这不是一个好主意。

关于 wardriving 的另外一件事情是：您的眼睛必须看着路上，在您驾驶车子的时候不要看您的计算机。带上一个朋友，在您驾驶时他操作计算机，或者在您准备捕获信号之前将车先停下。撞倒了漂泊的步行者或者撞到了另一辆车子，您一天的努力就白费了。

13.4　不用嗅探工具搜索—— Warchalking

warchalking 究竟是确定可接入的 Wi-Fi 信号的一种新标准还是昙花一现，目前还不得而知。无论是哪种情况，它都是一种有趣的现象。作为传统的流浪汉在门柱上留下的用来提示后来者的标记(例如，用来表示“这儿有个好心的夫人”或“如果您在这做事就有饭吃”的符号)在高科技上的扩展，warchalking 符号被认为可以用来标记当地有 Wi-Fi 信号存在，并指导知道密码的人如何连接到网络。

最早由英国的 Web 设计者 Matt Jones 在 2002 年夏天建议的 warchalking 符号(如图 13-1 所示)迅速在全世界传播开来。这种符号很简单。一个封闭的圆圈表示一个封闭的网络；两个背对背的半圆表示可访问(“开放”)的网络；一个圆圈里面放个 W 表示有 WEP 加密的网络。网络的 SSID 标在符号的上面，带宽标在下面。

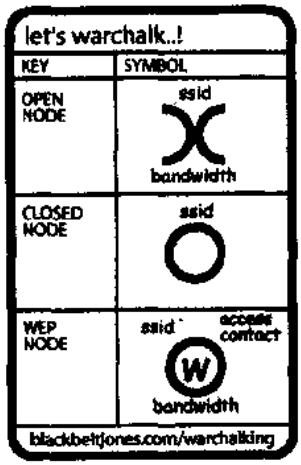

图 13-1　Matt Jones 的原始 Warchalking 符号

Warchalking 具有现代故事巨片的所有要素——奇异的技术怪人使用独特的图形维持着他们隐藏着的业余爱好——所以全世界很多的报纸和广播都报道了这一奇怪的新行为。但是实际上，要想知道 warchalking 标记在玩过新鲜后会不会真的变成通用的标准现在还为时过早。大多数私有网络的所有者并不想让外人知道他们的网络，公共网络的管理者通常只在他们商店的橱窗里或者他们自己的地方用简单的文字说明。除了社区网络使用者，大部分 Wi-Fi 接入点的管理者都不鼓励外人使用他们的网络。

然而，如果您想玩这个游戏，也是很容易的。只需在带着您的 wardriving 工具箱的同时再带一块石灰石(学校用来填坑的运动场上用的石灰石最好)，当您发现一个无线网络信号的时候，就在墙上或人行道上做个不显眼的标记。如果知道 SSID 和带宽的话也标上它们，然后继续往前走。不要用油漆或任何其他永久性的标记——如果财产的所有者想涂去标记，应该让他们能够不费很大劲就能够做到。

如果您发现已经有这种信号存在，那么这是您找到了一个可以尝试建立无线连接的好地方的不错提示。但是不要期望找到很多的 warchalking 标记——杂志对这种现象的报道可能多于实际的做这种标记的人。当您漫步在圣何塞市区或伦敦市中心时，如果确实发现了某个符号，您可以指着它告诉您的朋友那是什么意思，让他们加深印象。

通常，游击式联网或 wardriving，或者任何您想叫的称呼，是指类似于监听您的邻居的无绳电话的那些行为中的某一种。那是一种娱乐，但未必是一种礼貌的行为。是的，您可以解释说某个人傻到操作一个未受保护的无线网络应该受到被其他人使用的惩罚或者带宽正好就在那附近让人占用，但是让网络的所有者(或者当您在线时走过来敲您车门的那个有礼貌的警察)确信您的意图是值得尊敬的，并且没有对任何人造成伤害是不太可能的。即便这可能是事实。

如果您把 wardriving 当成一种无益的业余爱好，就像那些带着无线电扫描设备到铁路装货的地方窃听火车调度员和每个火车司机之间对话的人那样，或者像那些带着一本工作簿(上面列出了他们所曾见到的每个物种)的观察鸟类的人一样，那么这可能是完全无害的。但是当您越过界限实际建立了一个未授权的连接时，您应该确定的知道自己在做什么——偷取带宽——并且准备承担后果。

本章到此结束，下一章将从另一方面来看看游击式联网：将讨论无线网络的安全以及将熟悉本章内容的人拒绝在您的网络之外的问题。

第14章　无线网络安全

必须强调指出，无线网络是不安全的。对于很多用户而言，在大部分时间里无线网络是足够安全的，但是 Wi-Fi 网络绝对的安全保密是不可能的。

一个简单的事实是无线网络采用带有明确定义的字符集的无线信号，因此如果某个人愿意花费足够多的时间和精力来监控这些信息，他很可能找到一种截获和读取包含在信号中数据的方法。如果您通过一个无线连接传送秘密信息，那么窃听者就可以复制这些数据。信用卡号码、帐户密码和其他个人信息都很容易遭受攻击。

加密和其他安全措施可以在一定程度上增加窃取数据的难度，但是这些方法并不能提供一种可以完全防止专业侦听的保护措施。正如任何警察都会告诉您，各种锁只可以防范诚实的人士，但是老练的窃贼却知道如何打开它们。可以在 Internet 上方便地查找到用于破解 WEP 加密的完整工具集。

更为严重的情况是，许多网络管理者和家庭无线用户并没有采用加密和其他构建于每个 802.11b 接入点和网络节点的安全特性，从而给网络入侵者敞开了进入网络的门户。在许多城市和郊区商业区以及相当数量的居民区中，注册并进入到未受保护的专用网是可能发生的。在 2001 年春季，旧金山大事记报道说，网络安全专家通过使用安装在旧金山商业区的一个有篷运货汽车顶上的有向天线，在每个街区平均能够登录到 6 个无线网络。目前，这个数量可能会更大。一年后，一些微软公司的员工进行了一次非官方的试验，它们在西雅图外的郊区发现了超过 200 个未受保护的开放接入点。此外，Tully 咖啡店的经营人员也报告过，他们发现许多顾客通过在街对面的 Starbuck 商店的接入点来登录到 Wi-Fi 网络。

做一道如下的数学题：您的接入点的覆盖方向是全方位的，其范围大于或等于 150 英尺，因此信号的传播范围很可能超过了您的地界线(或者是住宅的围墙)。因此一个在此建筑物隔壁或街对面的网络设备很可能可以检测到您的网络，同理，一个停放在街上的汽车内的笔记本电脑或 PDA 均可以检测到您的网络。如果您不采取一些预防措施来保护网络，网络设备的使用者就可以登录到您的局域网上，从而从您的服务器中窃取文件，并且使用流媒体视频或多人游戏来阻塞您的 Internet 连接。

了解到我们正在讨论针对无线网络的两种不同的安全威胁是非常重要的，第一种威胁是指外部人员在您不知道的情况下，或者是未经您的许可就连接到您的网络；第二种威胁是指一个专业的窃听者可能窃取您发送和接收的数据。每种威胁都代表一种不同的潜在问题，并且需要不同的预防和保护措施。尽管当前没有工具可以提供彻底的保护措施，但是采用这些安全工具可以加大临时入侵者入侵网络的难度，并且由于这

些安全工具唾手可得，您可以使用它们。

使用无线网络必须在安全和方便上进行折衷，无线网络连接的明显优势在于它可以从一个便携式计算机或隔离位置快捷和方便地接入网络，当然这也是有代价的。对于大多数用户而言，该代价低于无线操作带来的好处。但是，正如您在大街上停放汽车时会锁住车门一样，也应该采取类似步骤来保护网络和数据。

14.1　保护网络和数据

作为一个无线网络的操作员，您应该采取什么措施来防止外部人员入侵呢？您有两个基本的选择：您可以接受 802.11b 网络并不完全安全这一事实，它只是通过采用内在的网络安全特性来减少入侵者攻击的可能性；或者您可以忽略该网络内在的安全工具，而使用一个防火墙来隔离无线网络。

显而易见的是，802.11b 协议内在的安全特性不足以在任何时间内保护全部的无线数据。如果您在贸易杂志上阅读了有关无线安全的文章，并且参与了在线论坛的讨论，那么您就很容易相信 Wi-Fi 网络是非常不安全的。但是这可能是夸大了对网络的真正威胁。记住，大部分距离近到可以窃听您的消息或者闯入您网络的人并不只是坐等您传送数据。老实说，通过您网络的大部分数据都是令人厌烦的数据，但是在每个 Wi-Fi 网络中都存在可用的加密工具，因此，您确实应该使用这些工具。

更加严重的安全威胁并不是攻击者窃听您在网络上传输的消息，而是攻击者会创建到您网络的连接，并且读取存储在网络中其他计算机上的文件，或者在您不知道或没有许可的情况下使用您的 Internet 宽带连接。

因此，采取必要的步骤来维护您对网络的控制是很有意义的。如果您选择实现 802.11b 的安全性，下面是一些需要采取的特定步骤：

- 尽可能将您的网络接入点放置在建筑物的中间，并且不要靠近窗户，以减少您的网络信号的覆盖范围，使其不会超过建筑物墙壁的距离。
- 使用包含在所有 8.02.11b 网络节点中的 WEP(有线等同隐私，Wired Equivalent Privacy)加密功能。如果拥有充足的时间和合适的设备，WEP 密钥并不难破解，但是加密的数据包比没有加密的数据更加难以读取。本章的后面将有更多关于 WEP 加密的信息。
- 经常更换 WEP 密钥。从数据流侦听出 WEP 加密密钥需要花费一定的时间，每当更换密钥时，试图窃取您数据的攻击者都不得不重新开始侦听密钥。每个月更换一到两次密钥是很有必要的。
- 不要将 WEP 密钥存储在正被使用的网络上，这一点看起来很容易做到，但是在一个广泛分布的网络中，您很可能将 WEP 密钥存放在一个私有 Web 页或文本

文件中。切记不要那样做。

- 不要使用电子邮件来分发 WEP 密钥。如果一个入侵者已经窃取了帐户名和密码，那么它可以在您的合法用户获得之前接收到带有新代码的消息。
- 在内嵌于无线网络的 WEP 加密的顶部增加另一个加密层，如 Kerberos、SSH 或 VPN。
- 不要使用您的接入点的默认 SSID，因为网络攻击者通常了解这些默认值。
- 更改 SSID，使其不能标识您的业务或位置。如果一个入侵者检测到一个称为 BigCorpNet 的标志，并且它们发现了在街对面的 BigCorp 公司总部，它们将会直接追踪到您的网络。同样对于一个家庭网络，如果您屋外的信箱侧面上印有 Perkins 字样，那么不要将您的网络叫作 Perkins。
- 不要使用一个使您的网络听起来好像包含了某些奇怪内容的 SSID，您应当使用一个令人厌烦的名字，如“网络”，或者是一组杂乱的字符串，如 W24rnQ。
- 更改您接入点的 IP 地址和密码。大部分接入点配置工具的出厂默认密码都容易得到(对于不同的制造商，它们经常是相同的——提示：不要使用“admin”)，因此它们甚至不能防止您自己的用户，更不要说那些试图利用您的网络来获得某种收益的未知入侵者。
- 如果这是一个可选项，请关闭您接入点中的“广播 SSID”特性，该特性可以接受来自没有正确 SSID 的客户端连接。尽管关闭此选项不能保证您的网络是隐蔽的，但是它将起到一些作用。
- 如果可能，启动您接入点内的访问控制特性。访问控制功能限制将您的网络连接到带特定 MAC 地址的网络客户端，接入点将会拒绝与地址不在列表中的适配器相关联。如果您想允许访问者使用您的网络，该特性可能不太实用，但是对于一个家庭的或小的业务网络，这是一个非常有用的工具，因为您知道所有潜在的用户。与“广播 SSID”选项类似，该选项不能确保网络安全，但是它没有什么坏处。
- 通过从建筑物外尝试访问您的网络来测试网络的安全性。携带一个运行嗅探程序的笔记本电脑，如 Network Stumbler 或网络适配器的状态实用程序，然后从建筑物旁走开。如果您可以在一个街区外的地方检测到您的网络，入侵者同样可以做到。记住，入侵者可能会使用高增益有向天线来扩展距离。
- 将您的网络看作是面向公共接入的网络，确保每个使用网络的人知道他们正在使用一个非安全系统。
- 限制您确实需要共享的文件，不要共享整个驱动器，并且对每个文件共享均使用密码保护。
- 使用您用于一个有线网络的相同安全工具。最好的情况是局域网中无线部分的安全性不会高于有线部分，因此您应该采取所有相同的预防措施。在大部分情

况下，您的网络无线部分的安全性远低于有线部分。

- 考虑使用虚拟专用网(VPN，Virtual Private Network)来增强安全性。

一些计算机安全人士采用了不同的方法来处理无线网络安全性。它们接受这样一个事实：802.11b 网络是不安全的，因此他们甚至不使用该网络内在的安全特性。例如，位于加利福尼亚州的 NASA 的高级超级计算机部认识到“网络自身并不能提供可靠的身份验证和防止侦听”，并且“802.11b 安全特性...只会消耗资源，而不会提供任何真正的安全性”。因此，该部门禁止了所有的 802.11b 安全特性，取而代之的是他们自己的无线防火墙网关(WFG，Wireless Firewall Gateway)。WFG 是一个位于无线部分和网络其他部分之间的路由器，因此所有进入和离开无线设备的网络通信量(包括接入到 Internet 的流量)都必须经过此网关。

这种安全方法的另一个额外好处是它将每个信息包中的管理开销最小化，因为这些信息包不包括身份验证或加密选项。也就是说，这种方法减少了每个信息包的比特数，从而增加了在网络中传输的有效数据率。

其他无线网络操作员使用 VPN 来控制经由无线网关的接入。在一个用户可以在网络上做任何事情之前，VPN 在 IP 层 (而不是进行 802.11b 加密的物理层) 增加了另一个端到端的安全特性层。

网络安全涉及到两方面内容：网络管理员不希望未授权的用户干扰网络，而每个用户不希望任何人获取他们的个人文件。当登录到一个公共网时，您应该采取一些预防措施来防止网络中其他任何人读取您的文件。

在试图连接到一个公共网络之前，您应当关闭文件共享(File Sharing)。在 Win95、Win98 和 Windows ME 中，采用以下步骤来关闭文件共享：

(1) 在“控制面板”(Control Panel)中打开“网络”(Network)对话框。

(2) 单击“文件和打印机共享”(File and Printer Sharing)按钮。

(3) 在文件和打印机共享对话框中禁止“允许其他用户访问我的文件”(I Want to Give Others Access to My Files)选项。

在 Win2000 和 Windows XP 中，没有一个关闭文件共享选项的集中控制位置，因此您必须分别关闭每个共享。具体而言，采用以下步骤来关闭文件共享：

(1) 打开“我的计算机”(My Computer)窗口。

(2) 窗口中将会出现所有共享的驱动器和文件夹图标，这些图标下均有一个“服务”(serving)图标的手。右击图标并从弹出的菜单中选择“共享和安全”(sharing and security)选项将会关闭共享。

(3) 在网络选项中关闭“共享文件夹”(Share This Folder)。

(4) 单击“确定”(OK)按钮将会关闭对话框。

(5) 对每一个共享文件夹或文件重复以上过程。不要忘记共享的文档文件夹。

当您重新返回到您的办公室或家庭网络时，您将不得不取消以上过程来再次共享您

的文件。

另一个完全不同的安全问题是：窃听者监视在无线连接中传播的数据，并窃取传输中的机密信息。这种情况虽然不如攻击者接入网络并读取您的文件那样常见，但也时常出现。加密和其他安全工具可以使数据更加难以破解，但最好是将 Wi-Fi 网络作为一个蜂窝电话来对待：不发送包含机密信息的消息或文件。

14.2 802.11b 安全工具

802.11b 规范中的安全工具是不完善的，但是它们聊胜于无。即使您选择了不使用这些安全工具，了解这些工具是什么，以及它们如何工作仍然是必要的。

14.2.1 网络名(SSID)

正如第一章所讲述的那样，每个无线网络都有一个名字。在一个只包含一个接入点的网络中，网络名是指基本服务集 ID(BSSID，Basic Service Set ID)。如果网络包含多个接入点，网络名是指扩展服务集 ID(ESSID，Extended Service Set ID)。所有网络名的通用名称是 SSID，这是一个您在无线接入点和客户配置实用程序中经常会看到的一个术语。

当您为一个网络配置接入点时，您必须指定该网络的 SSID。网络中的每个接入点和网络客户机都必须使用相同的 SSID。在运行 Windows 操作系统的计算机上，无线适配器的 SSID 也应该是该工作组的名字。

当一个网络客户机检测到两个或多个带有相同 SSID 的接入点时，它将认为所有的接入点都是相同网络的一部分(即使这些接入点工作在不同的无线信道上)，并且它将与可以提供最强的或最清晰的信号的接入点相关联。如果由于信号干扰或衰落而使此信号的质量降低，客户机将设法转换到它认为在同一个网络上的另一个接入点。

如果具有交叠信号的两个不同网络具有相同的名字，客户机将认为它们都是一个网络的一部分，并且它将尝试执行从一个网络到另一个网络的切换。从用户的观点来看，这种误导的切换看起来好像是网络完全丢弃了它的连接。因此，每个可能与其他网络交叠的无线网络必须有一个惟一的 SSID。

违反 SSID 惟一性这一规则的网络是仅提供对 Internet 的接入，而不与局域网中的其他计算机或网络设备相连的公共网和社区网。这些网络经常拥有一个通用的 SSID，因此用户可以从多个位置检测和连接这些网络。

一些接入点，包括 Apple 机场基站和类似的 Orinoco 系统，都包括一个可以提供在“打开”接入和“封闭”接入之间进行选择的特性。当接入点被设为开放接入(Open

Access)时，它将会接受来自一个将 SSID 设为“任意值(ANY)”的客户端的连接，以及来自于一个被配置为与接入点本身的 SSID 进行对话的设备连接。当接入点被设为封闭接入时(Apple 称之为隐藏网络)，它只接受 SSID 与接入点中的某个 SSID 相匹配的连接。这是一种将一些入侵者拒之于网络之外的好方法，但是只有当网络中的每个节点均使用一个 Orinoco 适配器时才有效(Apple 机场卡是 Orinoco 适配器的一种私有标签版本)。如果其他制造商的适配器试图连接到一个封闭的接入点，即使 SSID 是匹配的，接入点也将会拒绝它。

网络的 SSID 提供了一种非常有限的访问控制形式，因为当建立一个无线连接时，您必须指定 SSID。一个接入点中的 SSID 选项总是一个文本字段，它将接受您愿意分配的任何名字，但许多网络配置程序(包括在 Windows XP 中的无线网络工具以及几种主要网络适配器附带的工具)自动检测和显示在它们信号范围之内的每个激活的网络 SSID。因此当您设法进行网路连接时，没有必要一定知道网络的 SSID。有时，配置实用程序(或者一个网络监视器，或类似于 Network Stumbler 的嗅探程序)能够在一个列表或菜单中显示每个临近网络的名字。例如，图 14-1 给出了 Network Stumbler 探测程序在西雅图-塔科马机场扫描的结果，其中，WayPort 为乘客终端提供服务，而 MobileStar 为全美航空公司贵宾(VIP)俱乐部提供服务(在进行此项调查前不久，MobileStar 被另一种服务所包括进去，因此网络的名字发生了变化，但是此项服务仍然存在)。

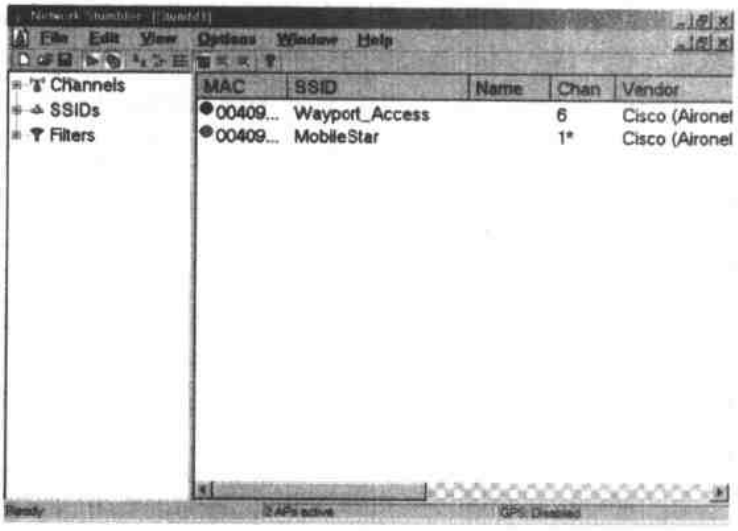

图 14-1　Network Stumbler 和许多配置实用程序显示每个临近无线网络的 SSID

每个接入点都具有一个默认的 SSID 设置，并且这些默认设置都是众所周知的，并且归档在网络探测社团内(例如可以查看：http://www.wi2600.org/mediawhore/nf0/wireless.ssid_defaults)。显而易见的是，不能在任何网络中使用默认值。

许多接入点具有一个可以隐藏 SSID 的选项，通常被称为“封闭的网络(Closed

Network)”或“隐形的网络(Cloaked Network)”。该选项有助于防止一些监听者检测您的网络名字，但是每当一个新客户机连接到您的网络，或者现有客户机获得的信号强度过弱，SSID 将被传送，并且类似于 Kismet 的软件可以检测到网络名。掩盖您的 SSID 可以降低临时观察者探测网络的概率，但是它并不能提供真正的保护。

14.2.2 WEP 加密

WEP 加密是每个 802.11b 系统中的一个选项，因此知道它如何工作是非常重要的，即使您选择不使用该功能选项。顾名思义，有线等同隐私(Wired Equivalent Privacy，WEP)协议的初衷是在无线网络上提供一种可以与有线网络的安全性相比的安全级别。但是这只是一种目标，因为有充分的证据表明，基于 WEP 加密的网络几乎与没有任何保护措施的网络一样容易受到攻击。WEP 加密可用于防止临时的探测者，但是对于专业入侵者而言，它没有特别效用。

WEP 加密可用于提供以下三种功能：它可以防止未授权的网络接入；它能够对每个信息包执行完整性检查；它可以防止数据被侦听者窃取。在一个网络客户端或接入点传送数据前，WEP 使用一个秘密的加密密钥对数据进行编码，然后当数据被接收后使用相同的密钥对信息包进行解密。

当一个客户机设法使用一个不同的密钥来与网络交换数据时，结果是杂乱的和可忽略的。因此，在网络中每个接入点和客户端适配器中的 WEP 设置必须完全相同。这听起来非常简单，但是可能会产生混淆，因为制造商会使用不同的方法来标识 WEP 密钥的大小和格式。从一种商标到另一种商标，该功能不会改变，但是相同的设置并不总是具有相同的描述。

1. WEP 密钥中的比特数

首先，一个 WEP 密钥或者是 64 比特，或者是 128 比特。128 比特的密钥更加难以破解，但是这也将增加传送每个信息包所需的时间。

不同制造商的实现之间会出现混淆，因为一个 40 比特的 WEP 密钥等价于一个 64 比特的 WEP 密钥，而一个 104 比特的密钥等价于一个 128 比特的密钥。标准的 64 比特 WEP 密钥是一个字符串，它包含一个内部生成的 24 比特的初始化向量和一个由网络管理者分配的 40 比特的密钥。一些制造商的规范和配置程序将其称为“64 比特加密”，但是其他制造商将其描述为“40 比特的加密”。无论哪种方式，加密机制是相同的，因此一个使用 40 比特加密的适配器与一个使用 64 比特加密的接入点或适配器完全兼容。

许多网络适配器和接入点也包含一个“强加密(strong encryption)”选项，它使用一个 128 比特的密钥(它实际上是一个带有 24 比特初始化向量的 104 比特密钥)。强加密

与 64 比特加密向下兼容，但它不是自动的，因此在一个包括 128 比特加密和 64 比特加密设备的混合网络中，所有的设备会按照 64 比特进行工作。如果您的接入点和所有的适配器都接受 128 比特加密，那么就使用一个 128 比特密钥。但如果您希望您的网络与只能识别 64 比特加密的适配器和接入点相兼容，那么就将这个网络设置为使用 64 比特密钥。

2. 密钥是 ASCII 还是十六进制

密钥的长度并不是设置 WEP 加密所遇到的惟一令人混淆的事情。一些程序要求密钥是由 ASCII 字符构成的字符串，而其他许多程序希望密钥是 16 进制的数字。此外，其他的一些程序还可以从一个可选的密码短语(passphrase)中生成密钥。

每个 ASCII 字符包含 8 个比特，因此一个 40 比特(或 64 比特)的 WEP 密钥包含 5 个字符，一个 104 比特(或 128 比特)的密钥包含 13 个字符。如果采用 16 进制，每个字符使用 4 个比特，那么一个 40 比特的密钥包含 10 个十六进制字符，而一个 128 比特的密钥包含 26 个字符。

图 14-2 中给出了用于 D-Link 接入点的无线设置屏幕，40 比特的共享密钥安全字段(Shared Key Security Field)使用 16 进制字符，因此它留有 10 个字符的空间。D-Link 程序在一个单独的字符串中一起运行所有的 10 个字符，但其他一些程序将它们分为包含两个字符的五组字符集，或者是包含五个字符的两组字符集。无论哪种方式，密钥对计算机而言是相同的，但是当它被分开时更加容易复制字符串。

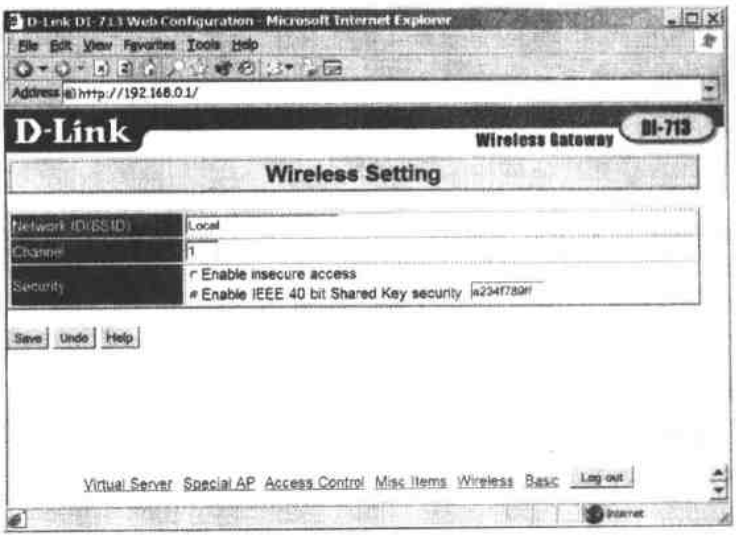

图 14-2　用于 D-Link 接入点的配置实用程序接受 16 进制格式的 WEP 密钥

许多客户实用程序，例如 Windows XP 中的 Wireless Network Properties 对话框(如图 14-3 所示)，提供了一个 16 进制或 ASCII 的选择，因此您能够使用与接入点中指定格式相匹配的格式。

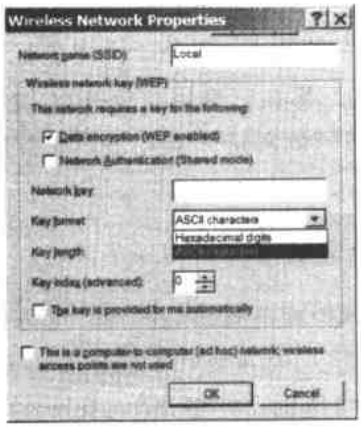

图 14-3　Windows XP 中的无线网络特性工具提供了选择 WEP 密钥格式的功能

密码短语是一个文本字符串；适配器和接入点可以自动将其转换为 16 进制字符的字符串。相比于 16 进制的杂乱信息，人们通常更容易记住实际的文字和短语，因此一个密码短语比一个 16 进制的字符串更容易分配。但是，只有当网络中所有的适配器和接入点均来自于相同的制造商时，密码短语才有用。

3. 任选项的概念

与 802.11b 配置实用程序中的任何其他事物类似，WEP 任选项(Options)的名称对于不同程序而言是不一致的。一些程序使用一组直观的选项，例如“启动 WEP 加密”，但是其他程序使用从正式的 802.11 规范中获得的技术术语。“打开系统”身份验证是“禁止 WEP 加密选项”的另一种表达方式。

一些接入点还提供一个可选的共享密钥验证选项，当一个网络客户机具有密钥时，它使用 WEP 加密，但是和其他网络节点通信时则采用未加密的数据。

4. 混合 16 进制密钥和 ASCII 密钥

当一些网络节点仅使用 16 进制，而另一些网络节点却要求使用 ASCII 密钥时，设置一个混合网络将变得更为复杂。如果网络是这样一种情况，您将需要遵循以下规则来设置 WEP 密钥：

- 将所有的 ASCII 密钥转换为 16 进制密钥。如果一个配置程序要求 ASCII 密钥，那么输入字符 0x(零后面跟着一个小写字母 x)，其后面跟着 16 进制字符串。如果您正在使用 APPLE 公司的 AirPort 软件，您将必须在一个 16 进制密钥的开始位置输入一个美元符号($)，而不是 0x。
- 确保您所有的密钥都确实有正确的字符数。
- 如果所有其他的办法都失败，阅读您的网络适配器和接入点手册的安全部分。在您的网络中可能存在一个或多个设备，这些设备具有一些您不了解的不明显

特性。

5. 改变 WEP 密钥

很多接入点和网络客户机适配器能够容纳四个不同的 64 比特 WEP 密钥，但是每次仅有一个密钥被激活，如图 14-4 所示。其他的密钥是备用的，这样就允许网络管理员可以立刻更新网络安全。支持 128 比特加密的适配器和接入点一次只保留一个 128 比特的密钥。

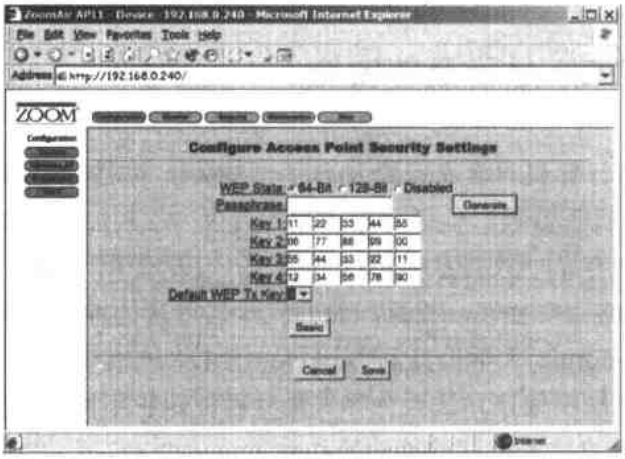

图 14-4　为了更换为一个不同的 WEP 密钥，需要改变默认值。真正的密钥应该比该示例中给出的密钥要更不明显

在一个正式使用 WEP 加密的网络中，应该定期更换 WEP 密钥。对于不携带紧急任务数据的网络而言，一个月更换一次密钥就足够了，但是更加重要的网络需要一周更换一次或两次密钥。另外，不要忘了将您当前 WEP 密钥的离线纪录保存在一个安全的地方。

在一个家庭的或小的企业网络中，您将可能亲自更改所有的 WEP 密钥。如果这种方法不实际的话，网络管理员或安全专家将通过纸便笺来分发新的 WEP 密钥，而不是使用电子邮件。对于使用 64 比特密钥的网络中的附加安全层，指导您的用户一次更改两个密钥(不是当前的默认密钥)。发送一个单独的便笺来通知用户哪个密钥将成为新的默认密钥，以及密钥改变在何时发生。

因此，一个典型的每周备忘录可能如下所示：

```
.....
Please enter the following new 64-bit WEP keys:
key 1:   XX XX XX XX XX
key 4: YY YY YY YY
.....
```

另一个一周后的备忘录将提供用于密钥 2 和密钥 3 的代码。

一个单独的备忘录内容可能是“我们的网络会在星期二午夜转换为密钥 3，请改变您的网络适配器中的默认密钥”。选择有尽可能少的人使用无线网络的时间段来进行密钥切换，因为当接入点的密钥改变时，任何活动的链路都可能丢弃它的连接，并且直到客户端适配器上的密钥改动后才能恢复连接。用户可以预先装载新的密钥作为当前激活密钥的替换项，当新的密钥变为有效时，用户只需简单地通过单击鼠标来改变这些密钥。

14.2.3 使用 WEP 是否足够安全

一些高等院校的计算机科学家已经发布了一些关于 WEP 加密的报告，他们反对使用 WEP 加密来保护机密数据。他们都指出用于定义 WEP 加密算法的加密理论和实践中的严重缺陷。这些专家一致同意遵循以下建议：任何使用 802.11 无线网络的人不应依赖 WEP 来保障网络的安全性，相反，他们应该采用其他方法来保护他们的网络。

加利福尼亚(California)大学伯克利(Berkeley)分校的一个小组已经知道了 WEP 算法中的许多缺陷，这些缺陷使该算法至少容易遭受以下四种不同的网络攻击：

- 使用统计分析方法来破解数据的被动攻击
- 构造加密的信息包使接入点错误地接受虚假命令的主动攻击
- 分析加密的信息包来构造一个字典，它可被用于实时自动地解密数据的攻击
- 通过改变信息包头文件来将数据转移到由攻击者控制的目的地。

伯克利分校的报告最后明确声明：有线等同隐私(WEP)不安全，该协议的问题在于它错误理解了一些加密的基本原语，因此以不安全方式组合了这些原语。

Rice 大学和 AT&T 实验室的研究人员也发布了他们自己对 WEP 加密的网络(http://www.cs.rice.edu/~astubble/wep)攻击的描述，并由此得出了一个近似的观点：“802.11 WEP 完全不安全”。他们定购和接收必须的硬件，建立实验床，设计他们自己的攻击工具，并且在不到一个星期的时间里成功捕捉到了一个 128 比特的 WEP 密钥。

无论是伯克利还是 AT&T 实验室的报告，它们都是由具有加密背景的技术专家写出，并且是写给同样的人看的。他们的结论很清楚，但他们的方法都是假设入侵者具有一些关键的技术知识。然而，对于缺少经验的代码破解者而言，同样容易找到各种工具。AirSnort(http://airsnort.shmoo.com) 和 WEPCrack(http://sourceforge.net/projects/wepcrack)都是监视无线网络信号，并且利用 WEP 算法中的弱点来提取加密密钥的 Linux 程序。

AirSnort 的开发者宣称他们的程序能够在大约两星期或更少的时间内成功攻破大多数网络。他们的技术手段是监视而不干扰网络信号，所以网络管理员不可能检测到

正在进行的攻击。他们发表了该程序来强调这个论点：如果能够容易地破解 WEP 加密，标准设置组将必须找到一种使其更加安全的方法，或者采用更加难以破解的方法来取代它。

要点：不断前进，并且对您的网络数据进行加密。加密的数据要比普通的文本传输更加安全，并且破解一个 WEP 密钥也需花费一定的时间，因此 WEP 确实增加了另一个(公认为较弱的)安全层，特别是当您频繁更换密钥时。WEP 加密对于防止专业攻击者所起的作用不大，但是它能够防止临时的网络监听者从街对面无意中发现您的网络，以及不定期经过的网络侦听。侵占一个未加密的网络更为容易(并且当前存在大量这样的网络)，因此检测到您的加密信号的攻击者很可能会将攻击目标转移到一个缺少保护的网络。

不断进行的改进

显而易见的是，如果一个安全机制的漏洞过大，那么该安全机制与根本不采用安全措施的结果几乎是相同的。对 WEP 加密成功的攻击，以及利用该协议安全问题的各种免费的可用工具使 Wi-Fi 联盟的成员开始认真考虑保护他们作为无线网络实际标准的特权。他们已经使用类似于“危机”此类的词语来描述对该问题的重视程度。他们希望对其进行完善和改进，以免有关安全攻击的不利宣传影响了他们精心营造和鼓励的对无线以太网设备不断增长的需求。

解决这些安全问题的新标准称为 802.11i。IEEE 802.11 标准委员会在该问题被广泛承认的几个月之前就开始讨论它。一个称为任务组 i(TGi，Task Group i)的委员会致力于提出一种改进的新安全规范，它将(希望)解决 WEP 加密标准中的所有已知缺陷。该工作组许诺新的安全工具将会自动工作，并且与不使用新的安全工具的旧硬件相兼容。该任务组的 Web 站点为：http://grouper.ieee.org/groups/802/11/Reports，在此站点中您可以找到与其相关的各种会议信息，并可以阅读一些技术文档。

Wi-Fi 联盟希望它的成员尽快开始使用 TGi 的修改版本，从而使他们能够在 WEP 酿成商业灾难之前缓解这种形势。一旦工程人员对这种解决方案感到满意，接入点和网络适配器的制造商也都会将这种新的安全方法集成到他们的产品之中，并且 Wi-Fi 联盟会将它添加到 Wi-Fi 验证测试套件中。软件和固件的更新会使现有的 802.11b 产品与新的 802.11i 产品兼容。

14.2.4　访问控制

大部分接入点包含一个可选项，它允许网络管理员限制对一组特定客户端适配器的

访问。如果一个 MAC 地址不在授权用户的列表之内的网络设备试图连接网络，接入点不会接受这个连接请求。因此该选项可用作防止入侵者连接到无线局域网的有效方法，但是它要求网络管理员保存一个用户适配器和 MAC 地址的完整列表。每当一个新用户希望加入网络，并且一个已确定的用户更换适配器时，必须由某人向此列表再添加一个 MAC 地址。对于一个家庭网或小型的办公网络，这种方法是可管理的，但是对于一个大企业网或校园网络，这将变成一项繁重任务。

每个接入点配置实用程序为它的访问列表使用不同格式，接入点提供的使用手册和在线文档提供了用于创建和维护一个访问控制列表的详细指南。

802.11b 标准没有指定用于一个接入点的访问控制列表的最大尺寸，因此这一数值是不确定的。一些接入点限制列表的尺寸为几十个数据项，但是另一些接入点，例如 Proxim Harmony AP 控制器可以支持多达 10000 个独立的地址。此外还有一些接入点对数量不加限制。如果您打算使用地址列表来控制对网络的访问，那么必须确保您的接入点可以支持足够大的列表以满足所有的用户，并且具有足够的扩展空间以满足将来增长的要求。根据经验所得，接入点至少应该接受当前您网络上两倍用户数量的 MAC 地址。

MAC 身份验证并不能防止所有攻击，因为可以在大部分无线卡上比较容易地改变 MAC 地址——攻击者所需要做的就是监视通信量足够长的时间来找到一个有效的用户，并且复制他的 MAC 地址。但是，与 WEP 类似，它是一种可以降低临时入侵者攻击网络的合理而有效的方法。

14.2.5 身份验证：802.11x 标准

鉴于 WEP 加密规范中的安全缺陷，许多无线网络设备制造商和软件开发者还采用另一种 IEEE 标准 802.1x 来向他们的无线网络增加另一个安全层。802.1x 标准定义了一种结构，它可以支持几种额外的身份验证形式，包括证书、智能卡和一次性的密码，所有这些验证形式都可以提供比内嵌于 802.11 中的访问控制更强的保护功能。在无线 802.11 网络中，一种称为健壮性安全网络(Robust Security Network)的技术构建于 802.1x 框架之上，它限制只有授权的设备可以访问网络。

大多数终端用户需要知道关于 802.1x 的两件事：首先，它内置于一些(但不是所有的)802.11b 硬件和软件之中，包括 Windows XP 和近来许多接入点产品提供的无线配置实用程序，因此它可以再提供一个潜在的安全层；第二，它仍存在严重的缺陷，一个专业网络攻击者可以利用这些缺陷来入侵无线网络。许多难懂的技术细节正由 Maryland 大学的两位研究人员进行分析，具体内容参见网址：

http://www.cs.umd.edu/~waa/1x.pdf。

看起来好像一种模式正在兴起，是这样吗？来自相关硬件和软件公司的工程人员聚集在 IEEE 特别工作组中，他们致力于开发另外一些新的网络安全工具，从而使他们的产品可以防止黑客、解密高手、窃听者和其他攻击者的攻击。几个月之后，某个大学或政府机构的一个独立的研究人员发现新的工具也存在严重问题，它会将受保护的数据泄漏给入侵者，并且也存在漏洞。同时，世界上大量贫穷的终端用户不得不尽可能快地跟上发展的步伐，但是他们的无线网络仍然不是完全安全的。

我们该怎么做？安全的无线网络是否是一个不能达到的理想？如果您将无线安全问题看作猫和老鼠的游戏，那么非常明显，老鼠(侦听者和网络解密高手)将是赢家。但是这些老鼠需要掌握高级的知识和设备来避开现有的加密和验证工具。可以将它想象为您房屋的前门：如果您将大门敞开，任何人可以进入房间并偷取您的东西，但是当您锁上门和所有窗户时，将会给夜贼的进入带来更大的困难。一个专家可以打开门锁，但是仍将花费大量的时间和精力。

14.3　防火墙

如果您接受这样的思想：WEP 加密和 802.1X 都不能为无线局域网提供足够的安全保护，那么下一步需要采取的步骤就是寻求另一种可以防止攻击者入侵您网络的方法。因此，您需要使用防火墙。

防火墙是一种代理服务器，基于由网络管理员建立的一组规则，它可以过滤所有经过它进出网络的数据。例如，防火墙可能会拒绝来自一个未知源的数据，或者是与特殊来源相匹配的文件(例如一种病毒)。或者，防火墙可能允许所有从局域网到 Internet 的数据通过，但只允许一些特定类型的数据从 Internet 进入局域网。在一个局域网中最常使用防火墙的位置是到 Internet 的网关，如图 14-5 所示。防火墙在局域网和 Internet 之间工作，它监视所有进入和流出的数据。这种防火墙的初衷是保护局域网中的计算机免受来自 Internet 的未授权访问。

在一个无线网络中，您也可以将一个防火墙放置在无线接入点和有线网络之间的网关处。该防火墙可以将网络的无线部分与有线局域网部分相隔离，因此已经将计算机连接到网络，但是没有得到允许的入侵者将不能使用无线连接访问 Internet 或局域网的有线部分。图 14-6 给出了防火墙在无线网络中的位置。

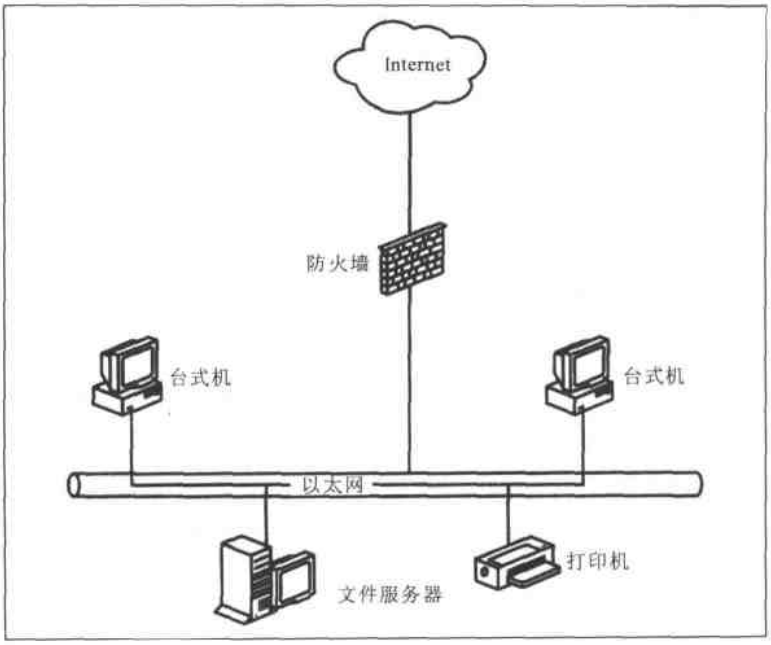

图 14-5　网络防火墙用于将局域网与 Internet 隔离

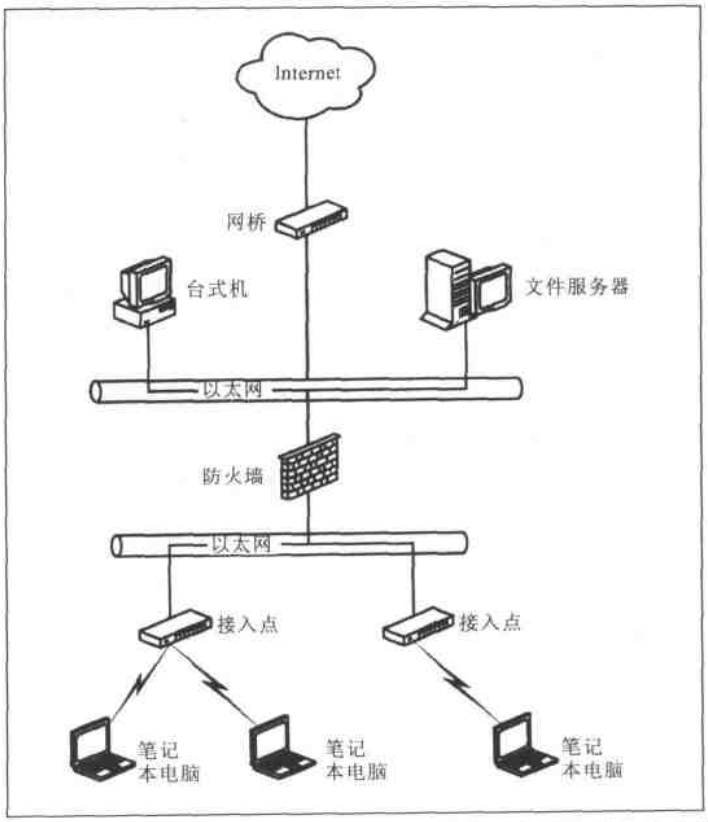

图 14-6　无线 LAN 中作为保护同一网络有线部分的网关的防火墙

14.3.1　阻止无线入侵者

大多数试图接入一个无线网络的人们并不关心此局域网上的其他计算机；他们致力于寻找到 Internet 的免费高速接入。如果他们不能使用您的网络来下载文件或连接到他们喜爱的网页，他们很可能会去寻找其他一些未受保护的无线热点。这并不意味着您应该将机密数据以文件共享形式存储在未受保护的计算机中，但如果您能限制或约束到 Internet 的访问，您可能会使您的网络对入侵者而言是缺少吸引力的。

无线网络中的防火墙可以执行以下几项功能：它作为一个位于无线网络和有线局域网的路由器或一个到 Internet 的直接连接；它可以阻止来自无线网络部分中未验证用户的所有通信量流向有线网络，但是它并不会干扰来自受信任用户的命令、消息和文件传输。一个合法用户可以连接到混合局域网中有线部分的网络节点或 Internet 上，但是一个入侵者将被防火墙所阻隔。

由于授权用户和入侵者均在防火墙的未保护端，所以防火墙不能彼此隔离无线节点。一个入侵者仍然可以获得相同无线网络中另一个计算机的使用权，并且可以读取共享的文件，因此，最好应取消任何连接到无线网络的计算中的文件共享。

一个用于无线网络的防火墙应采用一些验证来允许合法的用户通过网关，并拒绝其他任何人。如果基于内嵌于 802.11b 系统中 MAC 地址的访问控制以及 802.1x 中附加的验证机制不能满足要求，那么一个外部防火墙应要求每个用户在连接到 Internet 之前输入帐号和密码。

如果无线网络包括运行多个操作系统的计算机，那么您的防火墙必须使用一个可以工作在任何平台上的注册工具。实现这一功能的最简单方法是使用基于 Web 的验证服务器，例如包含在 Apache Web 服务器中的工具(http://httpd.apache.org)。

NASA NAS 中心使用一个专用服务器上的 Apache 来创建一个 Web 站点，它指导用户输入帐户名和密码。该服务器使用 Perl/CGI 脚本来比较输入的帐户名及密码与数据库中存储的信息，如果信息正确，它将指引服务器接受来自用户 IP 地址的命令和数据。如果用户名不在数据库中或密码不正确，Apache 服务器将显示一个“无效的用户名和密码”的 Web 页。

Apache Web 服务器可以作为一个 Unix 应用程序使用，它能够运行于一个使用早期 Pentium，或者甚至是 486 CPU 的旧型慢速计算机上。因此，经常可以反复使用日常不再使用的旧的破机器作为防火墙。Apache 应用程序和 Unix 操作系统都可以作为开放源代码的软件获得，因此您应该可以以非常低的代价来构造一个 Apache 防火墙。

如果更愿意使用 Windows，而不是 Unix，您有如下几个选项。您可以使用 Apache 的 Windows NT/2000 版本，或者使用一个商业实用程序，例如 Sygate 的无线监视程序(Wireless Enforcer)(http://www.sygate.com/products/sse/sse_swe_security.htm)。无线监视

程序和 Sygate 安全企业套件的其他元素一起工作，它们为每个授权用户分配和验证一个惟一指纹。如果入侵者尝试在没有正确指纹的情况下连接到一个接入点，网络会将他们拒之门外。

14.3.2 将您的网络与 Internet 相隔离

对无线局域网的攻击并不都是来自于空中。一个无线网络也需要使用类似于其他网络使用的防火墙来防止来自 Internet 的攻击。许多接入点包含可配置的防火墙功能特性，但如果您的接入点没有这些特性，网络应该包括一个或多个这样的防火墙：

- 运行于每个计算机之上的防火墙程序
- 充当网络防火墙的单独路由器或专用计算机
- 一个集成的安全套件，例如前一节介绍的 Sygate 套件

客户端防火墙程序提供了另一个防护措施来防止来自于网络外部的通过 Internet 的攻击。一些攻击来自于那些正寻求一种方法，从而可以读取您不愿被其他人看到的文件和其他资源的攻击者。其他攻击者可能希望利用您的计算机作为获得其最终目标的中继点，或者作为尝试进入世界上其他计算机的跳板，目的是使真正的攻击源更加难以标识。此外，还有一些攻击者传播病毒，或者使用真正的恶意程序来控制您的个人计算机，并且显示威胁消息。另外，一个具有大量未使用存储空间的未保护系统常常成为希望发布盗版软件、音乐和视频文件的黑客的攻击目标(他们不会将那些东西存放在自己的计算机上)。

Internet 上这样的愚人非常多：如果您安装了一个防火墙，它可以通知您外部的计算机试图连接到您的网络，那么每天您都可能看到多个入侵您网络的企图。

14.3.3 带有防火墙的接入点

在无线网络中使用最方便的防火墙是内嵌于接入点的防火墙。一些防火墙将无线接入点的功能和宽带路由器以及以太网交换机相结合，因此它们可以支持有线和无线网络客户。

正如您所知道的，网络路由器可以为标识局域网到 Internet 的数字 IP 地址和局域网内部标识单个计算机的内部 IP 地址之间提供地址翻译服务。防火墙一般将阻塞所有引入到网络主机的数据请求，但是当您希望使用局域网中一个或多个计算机作为文件服务器时，这将会产生问题。为了解决这个问题，防火墙可以包括一个虚拟服务器，它可以将某些种类的请求重定向到防火墙内正确的计算机上。

每一个到服务器的连接请求包含一个用于识别服务器类型的特定端口号。例如，

Web 服务器工作在 80 端口上，FTP 服务器使用端口 21，也就是说，这些端口号是接入请求的一部分。为了接纳接入某个服务器的请求，必须指导防火墙的网络地址翻译(NAT，network address translation)功能来将这些请求转发到局域网内一个特定的计算机上。在图 14-7 中，虚拟服务器被配置为使用本地 IP 地址为 192.168.0.17 的计算机作为 Web 服务器，并使用本地 IP 地址为 192.168.0.164 的计算机作为 FTP 文件服务器。表 14-1 列出了大多数常用的服务端口号。

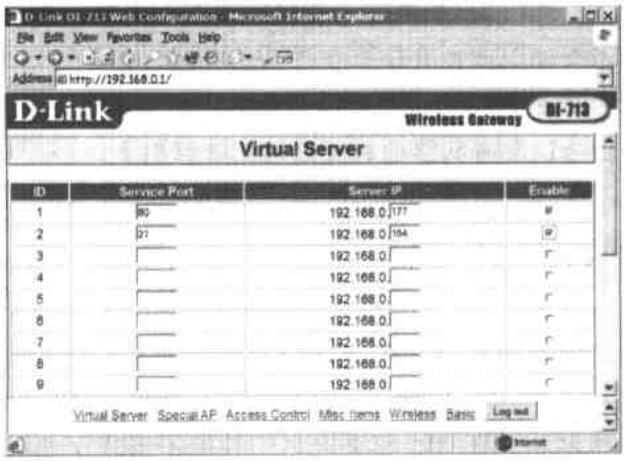

图 14-7　D-link 接入点将访问文件服务器的请求定向到网络中一个的特定计算机上

表 14-1　常用的 TCP/IP 服务端口号

端　口　号	Internet 服务
20	FTP-数据(FTP 默认数据)
21	FTP(文件传输)
23	Telnet
25	SMTP(发送的邮件)
37	Time
53	DNS(域名系统)
70	Gopher
79	Finger
80	HTTP(Web 服务器)
88	Kerberos
110	POP3(接收的邮件)
119	NNTP(网络新闻)
1863	Microsoft MSN Messenger
5190	AOL Instant Messenger
7070	RealAudio

此外还分配了上百个其他端口号，但是在实际使用中大多都看不到。端口号分配的官方列表可以参见网址 http://www.iana.org/assignments/port-numbers。

NAT 翻译假定每个虚拟服务器的 IP 地址不会随请求的变化而改变，一个地址为 192.168.0.3 的 Web 服务器在下一周不会将地址改动为 192.168.0.47。对于有线网络而言，这通常不是一个问题，但是在无线网络环境中，网络客户机会随时加入和离开网络，DHCP 服务器将会为每个新客户机自动分配下一个可用地址。如果一个客户机是其中一个网络服务端口的宿主，那么 NAT 可能无法找到该服务端口。当然这不是一个常见问题，因为大部分网络不会使用便携式计算机作为服务器，但是这种情况确实可能发生。一种解决方法是关闭 DHCP 服务器，并且为每个客户机分配一个永久 IP 地址，另一种解决方法是将服务端口传送到有网络的有线连接的计算机上。

14.3.4 防火墙软件

位于接入点和局域网有线部分之间接口处的无线网关防火墙能够防止入侵者使用您的网络来接入 Internet，作用于 Internet 连接的防火墙将可以阻止来自 Internet 的网络连接企图，但是在无线网络中还有必要采取另一种保护形式。如果某些人在没有得到允许的情况下访问您的无线局域网，您希望将他们排斥在同一网络上其他合法计算机的行列之外，在这种情况下，您需要在每个网络节点上运行客户端防火墙程序。

客户机防火墙在一个计算机的网络接口处工作，它与一个为整个网络工作的局域网或企业防火墙执行相同的功能：它检测连接到 TCP 服务端口的企图，并拒绝这些连接请求，除非它们与防火墙程序的一个或多个配置设置相匹配。

几种比较优秀的防火墙产品是作为共享件提供的，还有一些防火墙软件对于非商业用户也是免费的，因此可以方便的在您自己的系统上使用它们，并选择您最喜欢的软件。

下面给出一些 Windows 下的防火墙软件：

- ZoneAlarm(http://www.zonelabs.com/store/content/home.jsp)
- Tiny 个人防火墙(http://www.tinysoftware.com/pwall.php)
- Sygate 个人防火墙(http://www.sygate.com/products/shield_ov.htm)
- Norton 桌面防火墙(http://enterprisesecurity.symantec.com)
- Norton 个人防火墙(http://www.symantec.com)
- GFI LANguard(http://www.languard.com)

Unix 和 Linux 用户也可以选用多种防火墙软件，大多数这样的防火墙软件被编写为在常用作网关的单个防火墙计算机上使用，但是它们同样适用于保护单独的网络客户机。

在 Linux 中，防火墙是内核的一部分——ipchains 或 iptables。这两种形式的防火墙分别完整地归档在网址 http://linuxdoc.org/HOWTO/IPCHAINS-HOWTO.html 和

http://www.netfilter.org/unreliable-guides/packet-filtering-HOWTO/中。IP Filter 是一个为 FreeBSD 和 NetBSD 系统提供防火墙服务的软件包。IP Filter Web 的官方站点是 http://coombs.anu.edu.au/~avalon，另外在网址 http://www.obfuscation.org/ipf/ipf-howto.txt 中有非常优秀的解释性文档。该防火墙程序可以否决或允许任何信息包通过防火墙，它可以通过网络掩码或主机地址过滤信息包，建立服务端口限制，并且可以提供 NAT 翻译服务。

NetBSD/i386 防火墙是另一种免费 Unix 防火墙，它可以运行在任何具有 486 或更新的 CPU 和只有 8MB 内存的个人计算机上，NetBSD/i386 防火墙项目的主页是 http://www.dubbele.com。

PortSentry 是一种端口检测工具，它已被集成到几种广泛使用的 Linux 版本中，包括 Red Hat、Caldera、Debian 和 Turbo Linux。可网址 http://www.psionic.com/products/portsentry.html 上下载之。

14.4　虚拟专用网

虚拟专用网(VPN，Virtual Private Networks)通过隔离网络节点和其他网络通信量之间的连接来增加另一个有用的安全层。VPN 是一个加密的传输信道，它通过一个“数据通道”来连接两个网络端点。许多网络安全专家推荐使用 VPN 作为一种保护无线网络免受窃听和未授权用户进行访问的有效手段。下一章将进一步介绍关于建立和使用 VPN 的详细信息。

14.5　物理安全

至此，我们一直在讨论如何将电子入侵者拒于无线网络之外。通过使用还没有配置用于无线网络的现成设备，可以方便地访问该无线网络；当入侵者从一个授权用户窃取了一台计算机时，对网络的访问将更为容易。

笔记本电脑如果被窃贼偷走，事情将变得非常糟糕。如果窃贼使用被偷取的计算机来登录到一个网络，情况将变得更坏。作为网络操作员，您应该提醒您的用户，便携式计算机是窃贼非常感兴趣的目标，并且应该为他们提供一些保护计算机的指导。此外，您本身作为一个计算机用户，也应谨记相同的规则组。

第一个规则非常简单：不要忘了您正在携带一台计算机。这看起来是显而易见的，但是伦敦的出租车司机在六个月的时间内发现大约 2900 个笔记本电脑(和 62000 个移动电话！)遗留在他们的出租车上。此外，还有不计其数的笔记本电脑会被遗忘在飞机上、

旅馆房间内、地铁中和会议中心内。如果物主不经意离开的话，窃贼不需要偷就能获得用户的计算机了。

不要说明您正携带计算机这一事实。那些侧面印有大写字母“IBM”和“COMPAQ”的尼龙袋可能很流行，但是它们不如普通的公文包和传统的运输袋安全。

下一个规则是，当计算机没有锁在储物柜或存物箱时，您应将计算机拿在手上或背在肩膀上。稍微有所疏忽，高明的窃贼就会将您的计算机偷走。机场候机楼、铁路候车室以及旅馆休息室都是容易遭受快速偷窃的地方。如果您不得不在一个公共场合使用计算机，使用自行车链或钢制电缆将它安全地锁在一个不可移动的物体上。

不要将一个不安全的笔记本电脑整夜留在办公室内。

警惕机场的扫描器，让安全人员用手检查您的计算机，或者确保当计算机离开传输带时，您可以立刻取回它。两个协同作案的窃贼可以轻松地耽误您，并在您取回计算机之前将其拿走。如果某人设法从安检口偷走您的计算机，您应该大声叫喊并求助于保安人员。

确保您的计算机和类似于 PC 卡的松散部件在内部和外部都有财产标签。将您的名字、公司名称和电话号码都刻在网络接口卡和其他可移动部分上。一个称为“办公室财产安全跟踪”的公司(http://www.stoptheft.com)提供一种注册的安全电镀标签，它具有氰基丙烯酸盐粘合剂的粘性，需要超过 800 磅的压力才能除去这个标签，即使某些人去掉了标签，在标签处也将会出现一个印有“偷窃的财产”的不可擦除的化学刺字。

如果您能够说服用户在他们的计算上使用报警设备，那么将可以提高他们找回计算机的概率。TrackIT(http://www.trackitcorp.com)是一种两件套的报警设备，它使用一个钥匙链发射器，该发射器带有一个放在计算机袋内的微型接收器。当发射器距离接收器的距离超过 40 英尺时，接收器将发出 110 dB 的报警声，这一般会迫使窃贼丢弃偷取的计算机包装袋。

最后，将计算机型号和序列号列表保存在一个与设备本身相分离的地方，因为您需要这些信息来要求获得保险赔偿。

当您发现连接到您的无线网络中的一个计算机丢失或被偷窃时，您需要保护网络的其余部分。如果可能的话，您应该尽可能快地更换网络的 SSID、密码和 WEP 密钥。如果网络使用一个 MAC 地址列表来控制访问，您应该将被偷窃设备的 MAC 地址从授权的连接中删除。

14.6　与外部世界共享网络

如果您使用无线网络来提供到邻近区域或校园网的公共 Internet 接入，或者如果您希望允许客户和其他访问者连接到您的无线网络，那么您将不需要使用 WEP 加密或其

他安全工具来限制已知用户的接入。但是，您仍然应当考虑到安全问题。如果仅仅是因为您希望提供给人们一个到 Internet 的直接连接，这并不意味着您希望他们进入您网络的其他计算机中——因此有必要将无线接入点与网络的其余部分相隔离。

如果局域网中的所有本地节点都通过线路相连，那么最好的方法是将防火墙放置在无线接入点和有线局域网之间，它只允许接入点(以及通过无线链路连接到接入点的计算机)与 Internet 相通信，但是不允许它与有线局域网中的任何本地节点通信，如图 14-8 所示。

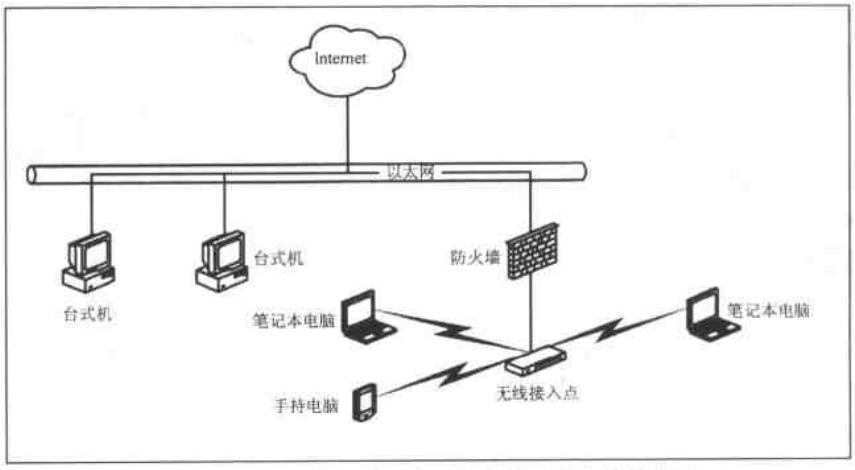

图 14-8　防火墙隔离网络的无线部分和其他部分

但是，如果您的一个或多个内部计算机使用无线连接，您需要保护它们不被外部攻击者使用网络的公共部分来接入。可以采用如下两种方法：在图 14-9 中，无线网络中的每个内部计算机均有一个软件防火墙，而图 14-10 给出了一个使用两个具有不同 SSID 的分离的无线网络系统，这两个无线网络均连接到相同的 Internet 连接点。一般来说，基本规则是采用一个或多个防火墙，将您网络的公共部分与不希望向外部世界每个人公开的计算机相隔离。

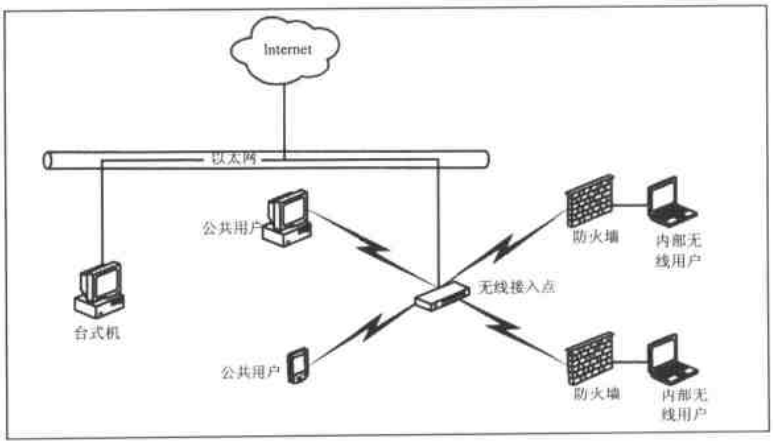

图 14-9　每一个内部无线计算机都包含一个软件防火墙

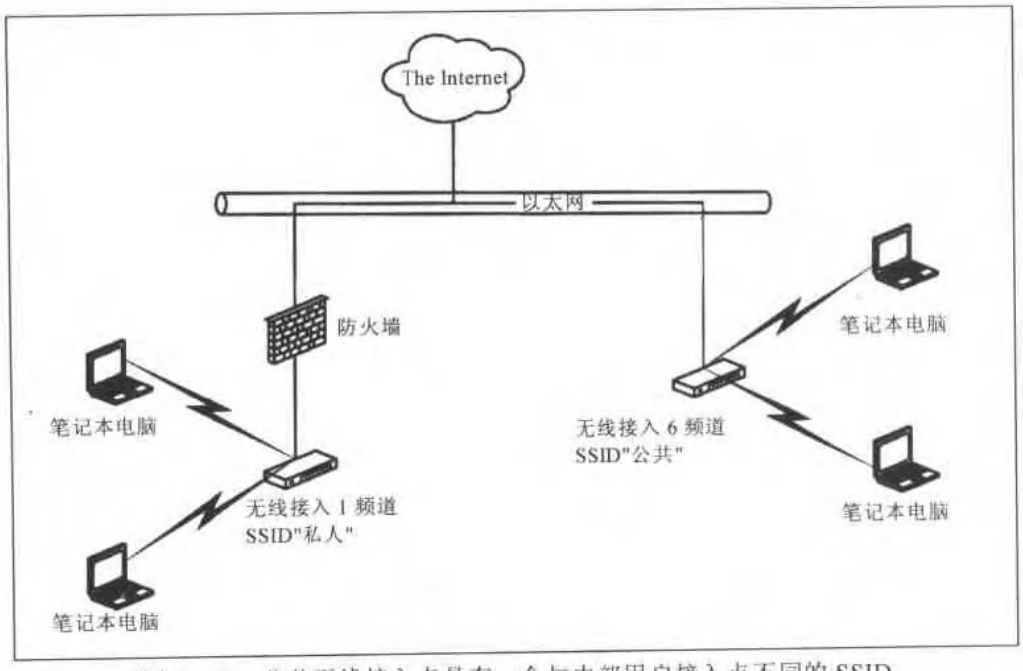

图 14-10　公共无线接入点具有一个与内部用户接入点不同的 SSID

第15章　虚拟专用网

IEEE802.11 规范中的安全工具并不够完善，它不能够保护通过无线网络的数据传输，那么应该采用什么样的替代方法呢？虚拟专用网(virtual private network，简写 VPN)能够向数据的传输增加另一种有效的安全形式，该数据从一个无线网络客户机传输到带网络连接的任何位置的主机。

VPN 使用“数据通道”通过加密的信道来连接一个网络的两个端点，端点可以是单个网络客户机和网络服务器、一对客户机计算机或其他设备，或者是到一对局域网的网关。通过公共网络(如 Internet)的数据完全与其他网络通信量相隔离。它使用登录和密码验证来限制只有授权用户可以接入 VPN；它对数据进行加密，从而使截获数据的入侵者无法识别数据；它采用数据验证来维护每个数据信息包的完整性，并且确保所有数据来源于合法的网络客户端。VPN 不仅仅是另一个加密层，它将端到端的数据路径与其他网络用户相隔离，因此未授权的用户不能获得它。VPN 的功能产生于 IP 层或者 ISO 模型的网络层，因此它们可以运行在 802.11b 协议的上面，该协议运行在物理层上。VPN 还可以跨越一个包括多种物理媒质(例如一条将数据传递到有线以太网的无线链路)的网络连接传递数据。换句话说，VPN 是一种端到端服务，而不考虑它正在使用无线链路、以太网电缆、普通的电话线还是以上类型和其他传输媒质的某种组合。VPN 是一种通道，它可以从一个网络端点扩展到另一个网络端点，而不用考虑使用何种媒质传送数据。因此它向只用于网络无线部分的 WEP 加密添加了另一个安全层(或者提供了一种可替换的方法)。

在传统的 VPN 中，一个远程用户可以登录到一个距离很远的局域网，并且能够获得与本地客户机相同的网络服务。VPN 常用于扩展企业网络到分店的连接，并可以从住宅或从厂区外的位置(例如客户或顾客的办公室)将用户连接到局域网。

通过 VPN 服务器连接的客户设备与同一个房间或建筑物内的客户设备一样呈现给(受 VPN 保护的)网络的其余部分。两者之间惟一的区别是来自于 VPN 的数据通过一个 VPN 驱动程序和公共网络进行传递，而不是直接从网络适配器移动到局域网。图 15-1 给出了到一个远程网络的典型 VPN 连接。

一个常规的有线 VPN 的所有安全优势同样也适用于通过无线链路的近程 VPN，以及起始于一个无线网络，并且将数据中继到一个远程服务器的远距离 VPN。下面是 VPN 的两种不同使用方式：本地 VPN 仅仅可以将客户机设备和接入点之间网络

的无线部分进行延伸；扩展的网络可以传送 VPN 编码的数据，它通过公共网络(例如 Internet 或拨号电话连接)，跨越过接入点，从而到达 VPN 服务器。

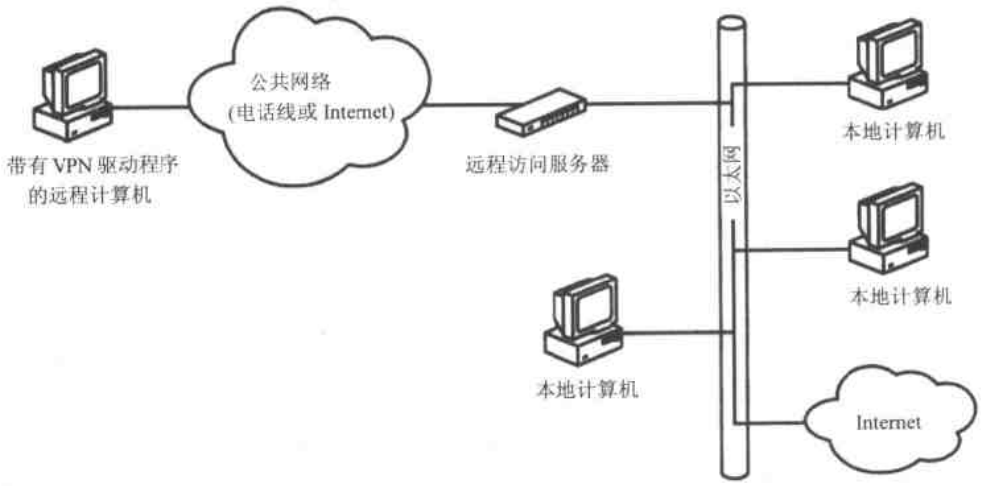

图 15-1　远程网络可以通过虚拟专用网连接到局域网

扩展的网络是传统的 VPN(一个通过诸如 Internet 等公共网络的 VPN)，它碰巧起源于一个无线网络客户机。相同的 VPN 也可以支持不包含无线部分的连接，以及来自于机场和咖啡馆的公共无线服务的注册连接。这是使用 VPN 的常规方法。

本地的近程 VPN 对于工作在无线网络上的人而言更具吸引力，因为它们向无线链路上添加了另一个安全层。由于在无线客户机和网络接入点之间传输的数据是加密的(使用一种比 WEP 加密更为安全的算法)，对于任何可能正在监听无线信号的第三方而言，这些数据都是不可识别的。另外，由于位于接入点的 VPN 服务器不会接受来自没有使用正确的 VPN 驱动程序和密码的无线客户机的数据链接，所以入侵者不能通过将一个假冒客户机与接入点相联系来闯入网络。

无线 VPN 的目标是保护位于客户机和接入点之间的无线链接，并且阻止未授权的用户。因此，隔离并加密的数据可能只需穿过一个房间，而不是成百或上千英里。当然，接入点还可以通过 Internet 将 VPN 编码的数据中继到位于另一个位置的网络主机。

图 15-2 给出了到一个 VPN 的无线连接。VPN 服务器位于无线接入点和主机局域网之间，因此通过网络的无线部分传输的所有信息包都被加密。为清楚起见，该图中的 VPN 服务器是一个分离的部件，但是在实际中，将 VPN 的安全性添加到一个无线局域网的最常用方法是采用集成了 VPN 功能的路由器或网关。具有 VPN 功能的路由器可以从多个供应商处获得，包括 Alvarion、Colubris 和 Nexland。

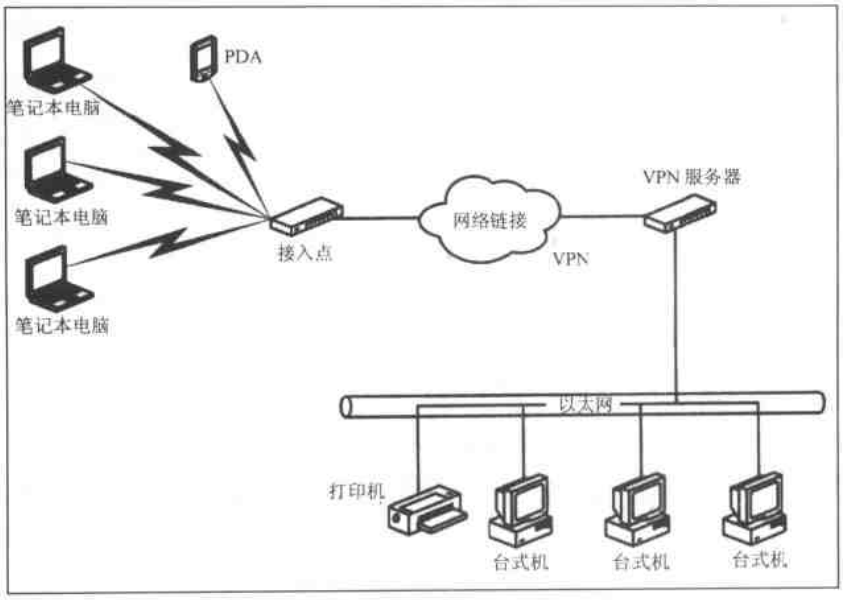

图 15-2　VPN 在无线网络和 Internet 网关或局域网之间提供了安全连接

15.1　VPN 方法

VPN 通过一个或多个中间网络将数据转移到另一个网络中的目的地。VPN 的通道客户机通过添加具有路由信息的新报头来封装现有的数据信息包或帧，路由信息指导数据信息包或帧如何到达 VPN 的端点。通过中间网络的传输路径称为通道，在通道的另一个端点，VPN 服务器去除通道头，并且将数据转发到下一层报头指定的目的地。通道的具体形式对数据而言没有任何区别，因为数据将通道看作为一个点到点连接。

通道头可以采用多种形式。VPN 中最常用的形式包括点到点通道协议(PPTP，Point-to-Point Tunneling Protocol)、第二层通道协议(L2TP，Layer Two Tunneling Protocol)和 IP 安全(IPSec)模式。PPTP 和 L2TP 可以通过 IP、IPX 和 NetBEUI 网络传递数据；IPSec 被限制用于 IP 网络。另外，客户机和服务器必须使用相同协议。

在 PPTP 和 L2TP 中，客户机和服务器在开始交换数据之前必须为每个传输配置通道。配置参数包括通过中间网络的路由以及加密和压缩规范。当传输完成时，客户机和服务器终止此连接并关闭通道。

在 IPSec 网络连接上，客户机和服务器在开始交换数据之前必须以单独的事务处理形式建立通过中间网络的通道。

以上这些协议中的每一种均具有相应的优点和缺点，但是它们都能够在一个无线网络客户机和接入点之间创建一条安全连接。三种协议之间的区别体现在技术上，而不是在应用上。您可以在名为《Virtual Private Networking in Windows 2000: An Overview》

的白皮书中找到所有三种协议内部操作的完整解释，该书可以从网址 http://www.microsoft.com/windows2000/docs/VPNoverview.doc 上在线获得。

15.2 VPN 服务器

VPN 服务器可以是一个 Unix 或 Windows 服务器的一部分，或者是内嵌于单独网络路由器或网关中。如果您的网络已经使用了一个单独的计算机作为专用服务器，那么您就可以使用该计算机作为 VPN 服务器。但是，如果您的网络还没有一个完整的网络服务器，一个分离的硬件部件可能是更好的选择。

许多 VPN 设备制造商提供可以支持一种或多种 VPN 协议的路由器、网关和其他网络产品。每种产品都有不同的特性集，因此在准备使用之前，有必要测试打算在自己网络上使用的客户机和服务器的特定组合。虚拟专用网联盟(VPNC)正致力于指定一组互操作性测试和证书标准(非常类似于用于 802.11b 设备的 Wi-Fi 标准)。VPNC 的 Web 站点 http://www.vpnc.org，列出了已经通过互操作性测试的各种产品，此外该网站还提供有关 VPN 产品完整列表的信息源的链接。

15.2.1 为无线 VPN 配置 Windows 服务器

如果您正在使用 Windows 服务器，PPTP 可能是最方便使用的协议，因为它初始时为一个 Microsoft 规范。许多 Windows 版本中都为 PPTP 提供了扩展支持，因此在不需要第三方软件的情况下也可以较为方便地配置 PPTP 客户机和服务器。Windows 2000 和 Windows XP 还支持 L2TP，因此 L2TP 可以作为另一个可以接受的选择。

用作 PPTP 服务器的计算机必须运行如下 Microsoft 服务器操作系统的一种：Windows NT Server 4.0、Windows 2000 Server 或 Windows XP Server。服务器还需要两个网络接口卡：一个连接到有线局域网或 Internet 网关，另一个连接到无线网络。连接到无线端口的接口卡通常直接连接无线接入点的以太网端口。

对于不同版本的 Windows 操作系统而言，在 Windows 服务器上安装 PPTP 的具体过程略微有所不同，但是一般的步骤是相同的。关于配置特定操作系统的特殊信息，可以咨询在线帮助屏幕、Microsoft 的资源工具包和其他的针对您操作系统的在线文档。以下部分描述了一般条件下的配置步骤。

1. 配置到有线网络的连接

到局域网或其他网络的连接是一个通过网络适配器的专用连接。用于此连接的网络连接配置文件必须包括分配给此连接的 IP 地址和子网掩码，以及分配给网络网关的默

认网关地址。

2. 配置 VPN 连接

VPN 连接通常是到一个或多个接入点的以太网连接。服务器上用于 VPN 连接的连接配置文件必须包括分配给此端口的 IP 地址和子网掩码，以及该网络使用的 DSN 服务器和 WINS 名称服务器的地址。

3. 配置远程访问服务器为路由器

服务器必须使用静态路由器，或者使用能够使每个无线客户端都可以被有线网络访问的路由协议。

4. 为 PPTP 或 L2TP 客户机启动和配置服务器

Windows 使用远程接入服务(RAS，Remote Access Service)和点到点协议(PPP，Point-to-Point)来建立 VPN 连接。路由和远程接入(Routing and Remote Access)服务启动 RAS，一个 VPN 连接需要如下 RAS 配置选项：

身份验证方法：加密的 PPTP 连接使用 MS-CHAP 或 EAPTLS 验证方法。

身份验证提供者：由 Windows 2000 安全机制或一个外部 RADIUS 服务器来验证网络客户机。

IP 路由：IP 路由和基于 IP 的远程接入必须被激活。如果有线网络充当无线客户机的 DHCP 服务器，那么 DHCP 必须被激活。

配置 PPTP 或 L2TP 端口：设置每个 PPTP 或 L2TP 端口来接受远程接入。

配置网络过滤器：输入和输出过滤器禁止远程接入服务器发送和接收不是起源于 VPN 客户机的数据。这些过滤器将拒绝发送到未授权的用户的数据，或来自于未授权用户的数据，因此那些入侵者将不能通过无线网络获得 Internet 连接(或者到有线局域网的连接)。

配置远程接入策略：每个无线客户机的远程接入权限必须设置为允许接入到 RAS 服务器。端口类型必须设置为正确的 VPN 协议(例如 PPTP 或 L2TP)，并且用于每个连接的配置文件必须包括正在使用的加密类型。在 Windows 中，包含以下三种加密增强选项：

- 基本加密：使用一个 40 比特的加密密钥
- 较强加密：使用一个 56 比特的加密密钥
- 最强加密：使用一个 128 比特的加密密钥

15.2.2　Unix 的 VPN 服务器

PoPToP 是用于 Linux、OpenBSD.FressBSD 以及其他 Unix 变体的 PPTP 服务器。

安装和其他相关使用信息，以及当前发行的版本都可从网址 http://poptop.lineo.com 上获得和下载。

所有 BSD 变体(包括 FreeBSD、NetBSD、OpenBSD 和 Mac OS X)都包括一个作为发布包一部分的 IPSec VPN 客户机和服务器。

Linux FreeS/WAN 是 Linux 的 IPSec 最流行的实现方式。可以到网址 http://www.freeswan.org 去下载该软件和相关的文档，并且可以访问 FreeS/WAN 用户社区。

如果您正在使用 Linux 防火墙，您可能希望将 VPN Masquerade(伪装)作为一个附加程序(如 PoPToP)的可替换选项。Linux 使用 Linux 内核中的 IP Masquerade 功能来使多个客户机共享一个 Internet 连接。VPN Masquerade 是支持 PPTP 和 IPSec 客户端的 IP Masquerade 的一部分。如何使用 Linux VPN Masquerade 的相关信息可以查询网址 http://www.linuxdoc.org/HOWTO/VPN- Masquerade-HOWTO.html。

15.2.3　带有内置 VPN 支持的网络硬件

运行 Linux 或一种 Unix BSD 版本的专用计算机可以作为一个廉价的 VPN 服务器；或者如果您出于其他目的正使用一个 Windows 服务器，那么该服务器也可以提供 VPN 支持，而仅需很小的成本，或者不需额外成本。对于相对简单的问题而言，一个功能完整的服务器常常是一个大且复杂的解决方案，这并不是最佳的选择。许多交换机、路由器、网关和防火墙设备也支持 VPN 功能。Cisco、3Com、Intel 和其他许多制造商生产的 VPN 产品比单独的计算机更易安装和维护。

在一个无线网络中，VPN 服务器不必像一个大型企业网中的服务器那样具有非常完善的功能。如图 15-3 所示，一个位于无线接入点和企业网有线部分之间的路由器可以同时充当 VPN 服务器。在一个家庭网络中，VPN 服务器可以工作在接入点和 DSL 或电缆调制解调器之间。

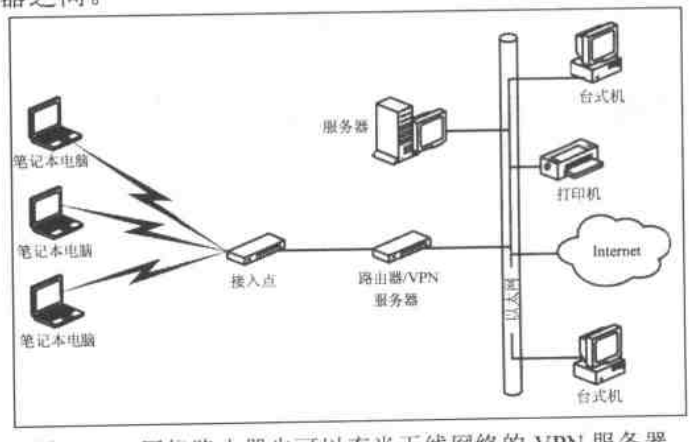

图 15-3　网络路由器也可以充当无线网络的 VPN 服务器

您也可以采用位于计算机和网络之间的单机 VPN 客户机硬件，但是在无线网络中，这种方式不实用，因为无线网络适配器通常总是直接插在计算机上。

15.3　VPN 客户程序软件

一个无线客户机通过到接入点的无线以太网链路连接到一个 VPN 服务器，操作系统将此连接看作一个局域网连接。为了通过该连接建立一个 VPN 通道，必须安装通道协议作为一种网络服务。

15.3.1　为 VPN 配置 Windows

大多数 Windows 版本中都支持虚拟专用网，但是它通常不是默认安装的一部分。因此，安装一个 VPN 客户程序的第一个步骤是安装此协议。在 Windows 用户版本中，应遵循以下步骤：

(1) 从 Control Panel 中选择 Add/Remove Programs。

(2) 在 Add/Remove Program Properties 窗口中打开 Windows Setup 选项卡。

(3) 在 Components 列表中选择 Communications，并单击 Details 按钮，将会打开如 15-4 所示的 Communications 窗口。

图 15-4　选择 Communications 组件列表中的 Virtual Private Networking 安装 VPN 协议

(4) 往下滚动组件列表来查找 Virtual Private Networking，选中该项目旁的复选框。

(5) 单击 Communications 和 Add/Remove Programs 窗口的 OK 按钮。

(6) 按照计算机的要求重启计算机。

在 Windows NT 和 Windows 2000 中，遵循以下这些步骤：

(1) 从 Control Panel 中选择 Network 选项。

(2) 在 Protocol 选项卡页面中，单击 Add 按钮，将会打开 Select Network Protocol 对话框。

(3) 从 Network Protocol 列表中选择 Point to Point Tunneling Protocol 并单击 OK 按钮，Windows 会装载 PPTP 文件。

(4) 当出现 PPTP Configuration 窗口时，选择您希望在此客户程序上支持的 VPN 设备数量。在大多数情况下，一个无线客户机使用一个设备就足够了。

(5) 在所有打开的窗口中单击 OK 按钮。

(6) 重新启动计算机来激活 VPN 客户程序。

(7) 为了将 VPN 客户程序添加为一个远程接入服务(RAS)端口，再次打开 Control Panel 并选择 Network，选中 Services 选项卡，并且选择 Remote Access Service 选项。

(8) 单击 Properties 按钮以打开 RAS Properties 对话框。

(9) 单击 Add 按钮来打开 Add RAS Device 窗口。

(10) 如果 VPN1-RASPPTPM 不可见，打开设备的下拉式列表，选择 VPN1-RASPPTPM 并单击 OK。

(11) 选择 VPN 端口并单击 Configure 按钮。选择指定无线网络端口的选项并单击 OK。

最后，您必须创建一个可以连接到 VPN 服务器的连接配置文件：

(1) 从 Control Panel 中或者 My Computer 窗口中打开 Dial-Up Networking。

(2) 双击 Make New Connection 图标，将会启动 Make New Connection Wizard。

(3) 在该向导的第一个屏幕上(如图 15-5 所示)的 Type a Name 字段中输入您的 VPN 服务器名称。

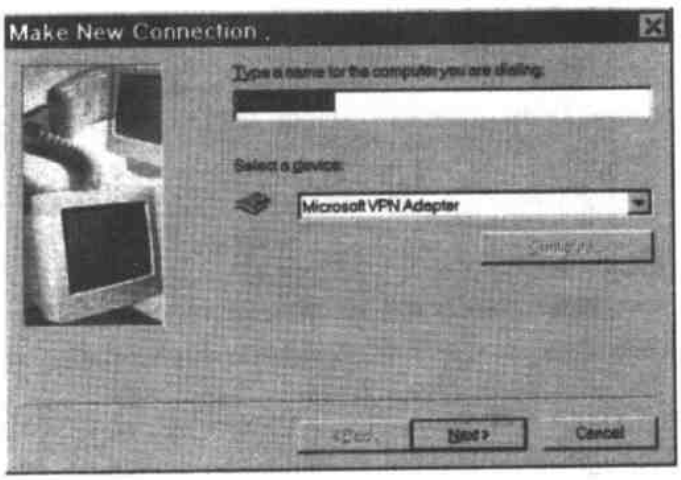

图 15-5　选择 Microsoft VPN Adapter 选项来创建一个 VPN 连接配置文件

(4) 打开 Select a Device 菜单并选择 VPN Adapter 选项，单击 Next 按钮前进到向导的下一个屏幕。

(5) 在 Host Name 或 IP Address 字段中输入 VPN 服务器的 IP 地址，单击 Next 按钮，向导将确认已经创建了一个新的连接配置文件。

(6) 单击 Finish 按钮来关闭向导，您应该在 Dial-up Networking 窗口中看到一个用于此连接配置文件的图标。

(7) 如果您打算经常使用 VPN 连接，创建一个到新连接配置文件的快捷方式，Windows 会自动将快捷键放置在您的桌面上。

在 Windows XP 中，使用向导可更为方便地完成整个过程：

(1) 从 Control Panel 中打开 Network Connections。

(2) 双击 New Connection Wizard 按钮。

(3) 当 Network Connection Type 窗口打开时，如图 15-6 所示，选中 Connect to the Network at My Workplace 单选按钮。

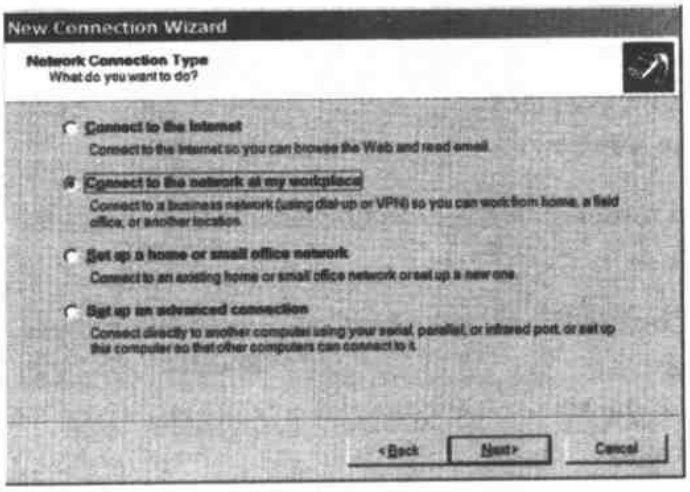

图 15-6　创建一个 VPN 链路的选项指定了到一个工作场所网络的连接，但它也适用于无线 VPN

(4) 在 Network Connection 窗口中(如图 15-7 所示)，选择 Virtual Private Network Connection 选项并单击 Next 按钮。

(5) 在 Connection Name 窗口中，输入无线 VPN 连接的名称，该名称会出现在到此连接的桌面快捷键中，然后单击 Next 按钮。

(6) 在 Public Network 窗口中(如图 15-8 所示)，选中 Do Not Dial 选项，因为您不需要通过电话线来连接，然后单击 Next 按钮。

(7) 在如图 15-9 所示的 VPN Server Selection 窗口中输入 VPN 服务器的 IP 地址。

(8) 单击 Next 按钮，然后单击 Finish 按钮以结束向导。

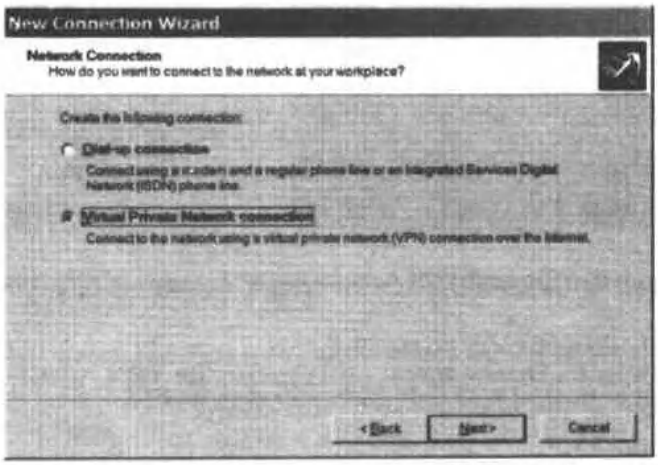

图 15-7　选择 Virtual Private Network 选项来创建一个 VPN 连接

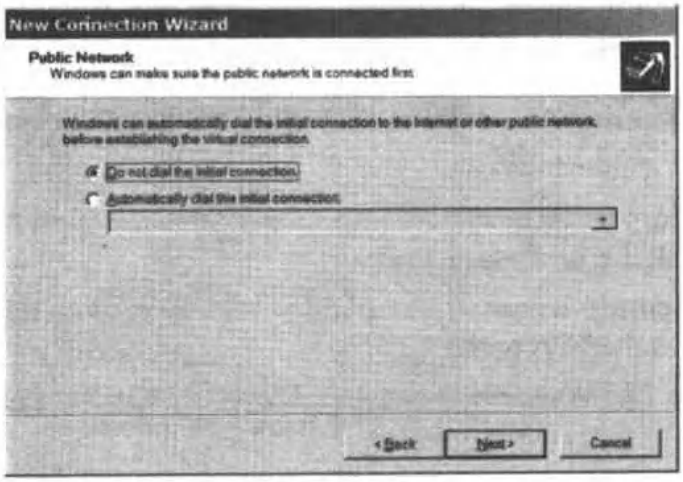

图 15-8　在一个无线网络中，VPN 不需要拨号连接

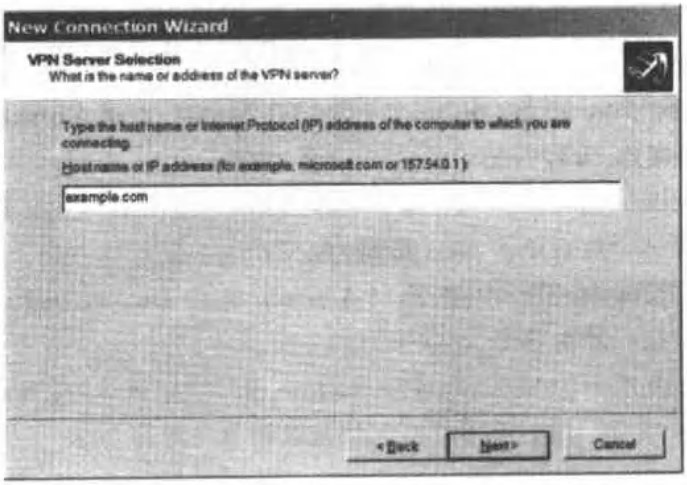

图 15-9　Host Name IP 地址用于识别无线链路另一端的 VPN 服务器

15.3.2　Microsoft L2TP/IPSec VPN 客户程序

在 Windows 2000 和 Windows XP 中，Microsoft 包括了带有 IPSec 的 L2TP 连接的客户程序。此外，用于 Windows 98、Windows Me 和 Windows NT Workstation 4.0 的类似客户程序也可以从 Microsoft 公司的网站免费下载。为了找到该程序，您可以到 Microsoft 的 Windows 2000 Tools 和 Utilities Web 页 (http://www.microsoft.com/windows2000/downloads/tools/default.asp)，并选择正确的链接。

15.3.3　在 Windows 中建立连接

一旦设置好 VPN 连接配置文件，您就可以方便地通过无线 VPN 链路将一个 Windows 客户机连接到主机局域网或 Internet：只需双击此连接配置文件的图标。Windows 将要求您输入用户名和密码，然后建立连接。

如果您的无线连接是您最常用的 Internet 连接方式，您可以将它设置为默认连接。这样，无论您何时启动了一个网络应用程序，例如 Web 浏览器或电子邮件客户程序，均会打开此连接。为了设置默认的 VPN 配置文件，应当遵循以下这些步骤：

(1) 从 Control Panel 中打开 Internet Properties 窗口。

(2) 单击 Connections 标签。

(3) 在 Dial-Up Settings 部分中，从列表中选择 VPN 连接配置文件，并且单击 Set Default 按钮。

(4) 单击 Settings 按钮，在 Dial-up Settings 部分中输入用于 VPN 服务器的注册号和密码。

(5) 选中 Dial Whenever a Network Connection Is Not Present 选项。

15.3.4　Windows XP 选项

Windows XP 提供了许多早期 Windows 版本中没有的 VPN 选项。为了设置这些选项，应当遵循以下这些步骤：

(1) 从 Control Panel 中打开 Network Connections 窗口，如果在桌面上已经有一个您的 VPN 连接的快捷键，可跳过这一步。

(2) 双击 VPN 图标，将会打开一个类似于图 15-10 所示的连接窗口。

图 15-10　在 Windows XP 中使用连接窗口来配置 VPN

(3) 单击 Properties 按钮，会打开您的 VPN 客户程序的 Properties 窗口，图 15-11 给出了 Properties 窗口的 General 选项卡。

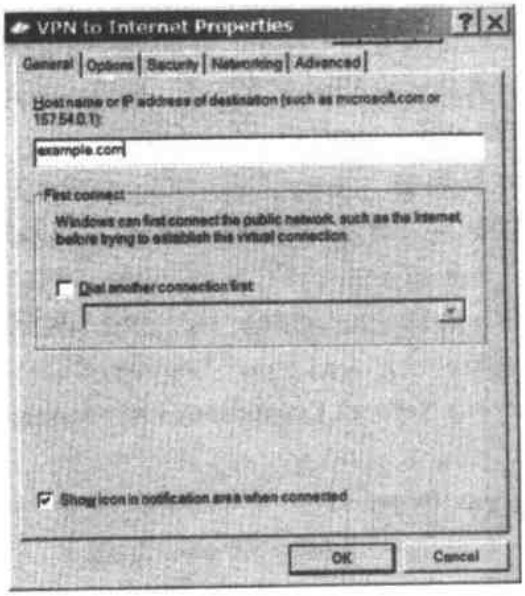

图 15-11　General 选项卡控制一个 VPN 连接的目的地

(4) VPN 服务器的 IP 地址应该出现在 Host Name 字段中，Dial Another Connection First 选项应被禁用。单击 Networking 选项卡来查看选项，如图 15-12 所示。

(5) 从 type of VPN 菜单中选择网络将使用的 VPN 服务器类型，如果您不知道 VPN 类型，选择 Aoutomatic 选项。

图 15-12　Networking 选项卡控制 VPN 的网络配置选项

(6) 从连接项目列表中选择 Internet Protocol(TCP/IP)，并单击 Properties 按钮来改变网络设置，这些设置包括您是否使用 DHCP 服务器，或 IP 地址和 DNS 的手工设置。

(7) 单击 Advanced 标签来显示如图 15-13 所示的窗口。如果您的网络还没有被一个防火墙所保护，打开 Internet Connection Firewall 选项，这将会保护无线客户机免受来自 Internet 的网络攻击。

图 15-13　Advanced 选项卡控制防火墙在 VPN 上的使用

Properties 窗口中的 Options 和 Security 选项卡控制通常不会变动默认设置的连接选项。需要改动安全设置的网络管理员应该指导它们的用户如何配置这些选项以符合网络的特定要求。

15.3.5　用于 Unix 的 VPN 客户程序

在一个运行 Unix 的计算机上使用 VPN 客户程序比在一个 Windows 机器上要复杂，因为客户机没有集成到内核中。因此，您必须找到一个可以与您正在使用的 Unix 版本和 VPN 协议共同工作的客户程序。没有一个程序可以提供一个通用的 VPN 客户程序，并且一些组合(例如工作在 BSD Unix 版本上的 PPTP)似乎根本就不存在。

1. PPTP-Linux

PPTP-Linux 是一个连接到 PPTP 服务器的 Linux 客户程序。该软件的开发者鼓励用户创建其他 Unix 版本的端口，但是他们自己的活动主要集中在 Linux 上。

PPTP-Linux 客户机项目的非官方网页是 http://www.scooter.cx/alpha/pptp.html。

2. IPSec 客户程序

Linux 用户可以选择以下几种 IPSec 实现方式：

- FreeS/WAN(http://www.freeswan.org)
- pipsecd(http://perso.enst.fr/~beyssac/pipsec)
- NIST Cerberus(http://www.antd.nist.gov/cerberus)

IPSec 包含在 OpenBSD 发行版本中，您可以在网址 http://www.x-itec.de/projects/tuts/ipsec-howto.txt 中找到一个说明如何使用它的指南。

FreeBSD 的 IPSec 实现方式可以在网址 http://www.r4k.net/ipsec 中找到。

关于 NetBSD IPSec 的信息，可参见网址 http://www.netbsd.org/Documentation/network/ipsec。

15.4　使用无线 VPN

当您设计 VPN 来保护您的网络中通过无线链路传输的数据安全时，准确了解 VPN 通道的端点位置是很重要的。如果 VPN 通道只通过无线链路，如图 15-14 所示，那么网络看起来就像没有使用 VPN 一样。但是，如果它的作用范围超出了无线接入点，从而通过一个广域网(如 Internet)进行传递时，如图 15-15 所示，无线网络客户机可能是位于另一个建筑物中一个局域网的一部分，或者是位于横跨大陆的途中。

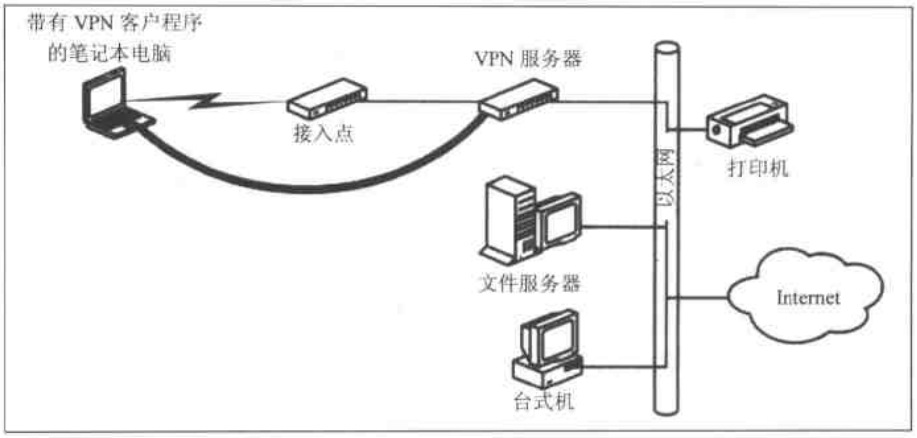

图 15-14　在接入点中，带有服务器的无线 VPN 保护数据通过无线链路，但是不能扩展网络

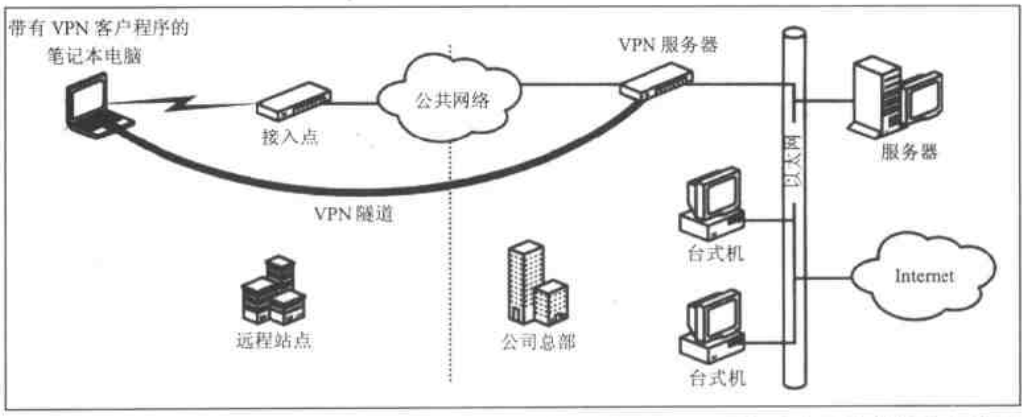

图 15-15　一个 VPN 可以包含无线链路，以及一个通过 Internet 到大企业网络的城市间连接

那么您的无线 VPN 应延伸多远呢？这取决于您希望网络实现的功能。如果您的无线网络用来支持您的办公室、工厂或校园的笔记本电脑和其他便携式计算机，将服务器放置在网络接入点和到您的企业局域网连接之间是有意义的。这将可以保护您的无线用户的数据，并且能够将未授权的用户拒于网络之外，但是它不会影响通过电缆将计算机连接到局域网的其他用户。

在家庭网络或小型商务网络中，接入点很可能连接到一个 Internet 网关路由器，它可以为办公室或家庭内的所有计算机提供 Internet 接入。如果接入点和网关是分离的设备，您可以将 VPN 服务器置于两者之间。但如果接入点和网关被组合在同一个盒子中，您将不得不在所有计算机上使用 VPN 客户程序，包括通过硬件连线接入网关的桌面型计算机，并且将客户机放置在网关和 Internet 调制解调器之间，如图 15-16 所示，或者可以忽略网关上的有线以太网端口，并在 VPN 服务器和 Internet 调制解调器之间添加一个新的集线器或交换机，如图 15-17 所示。

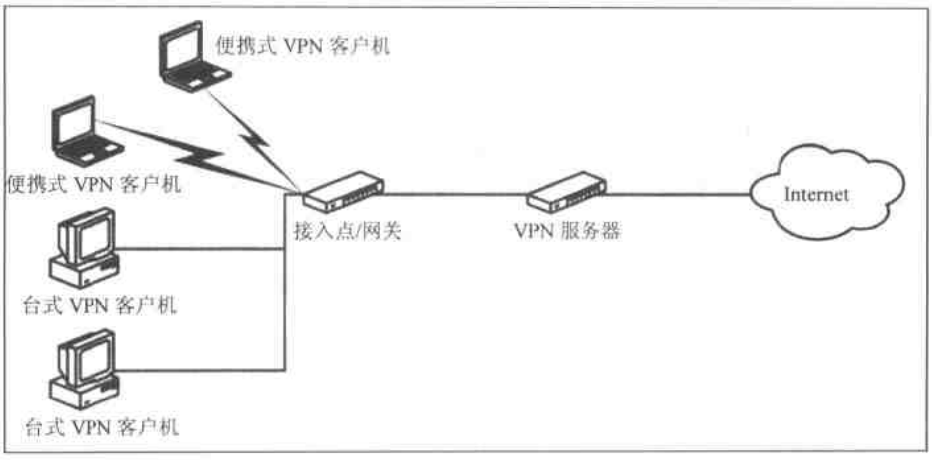

图 15-16　在一个小型局域网中，您可以在每台计算机上使用 VPN 客户程序

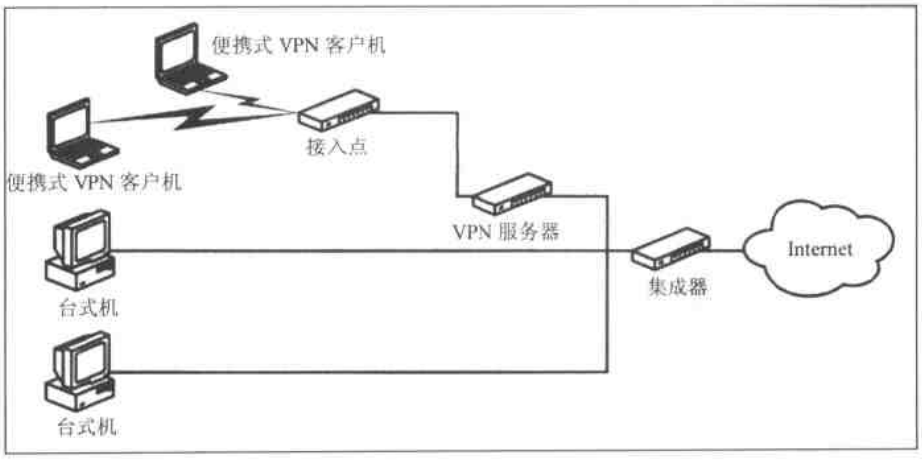

图 15-17　在这一网络中，VPN 仅保护无线链路

15.4.1　建立连接

如果大部分时间内您所使用的是具有 VPN 保护功能的无线局域网，您应该将 VPN 配置文件作为您的默认连接。无论何时您运行了一个网络应用程序，计算机都会设法通过 VPN 进行连接，除非您首先打开了一个不同的连接(如拨号电话线)。

为了在 Windows 中将连接配置文件设置为默认选项，打开 Dial-up Networking 窗口(在 Windows XP 中使用 Network Connections 窗口)，右击您希望选择的配置文件的图标，并从菜单中选中 Set as Default 选项的设置。

为了连接到一个不是默认设置的 VPN，双击该 VPN 连接配置文件的图标，您将会看到一个类似于图 15-18 所示的登录窗口。输入您的名字和密码，并单击 Connect 按钮。

如果 VPN 服务器认识您的账户，它将会建立连接。

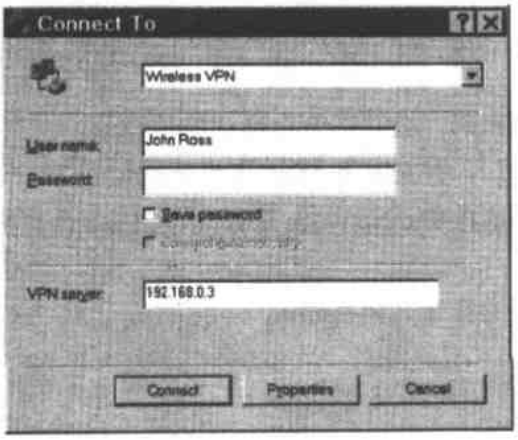

图 15-18　一个 VPN 连接通常要求登录名和密码

15.4.2　不使用 VPN

尽管通常使用 VPN 来保护您的无线数据，您有时可能希望在不使用 VPN 的情况下不受阻碍地发送数据。例如，您可以在您的办公室或家庭内使用 VPN，但是在一个机场、咖啡店或其他没有被 VPN 保护的场所使用同一台计算机时，可使用相同计算机和网络适配器来直接进行连接。

此外，控制网络的操作信道、SSID 和其他选项的配置程序都是源自于接入点中基于 Web 的实用程序。由于接入点在 VPN 通道内部，所以不可能通过 VPN 来向接入点发送命令。

记住，您可以在需要的时候使用 VPN，并且当您希望直接进行连接时可以忽略 VPN，这一点非常重要。

15.4.3　通过公共网络使用 VPN

当您在一个机场或会议中心通过一个公共网络将您的笔记本电脑连接到企业局域网时，您可以通过该局域网的网络连接到 Internet 和您的企业 VPN 服务器上。由于在初始化 VPN 连接之前，您将必须登录到公共网络上，因此除了使用的来自于您办公室的 VPN 连接配置文件外，您应该创建一个分离的“VPN via Public Network”连接配置文件。该配置文件应指向您的企业 VPN 服务器，但是它不应该是您的默认连接。

为了通过公共网络连接到一台运行 Windows 的计算机上，应遵循以下步骤：

(1) 正确打开带有无线网络适配器的计算机。

(2) 使用您的无线配置实用程序来选择您希望使用的公共网络。

(3) 启动 Internet Explorer、Netscape Navigator 或其他 Web 浏览器，您会看到公共网络的登录屏幕。

(4) 输入您的帐户和密码，公共网络会确认您的登录。

(5) 最小化浏览器窗口，并且打开 Dial-up Networking 窗口。

(6) 双击您的 VPN via Public Network 配置文件图标，计算机会通过 Internet 连接到您的企业局域网。

(7) 输入您的企业网的登录名和密码。

第16章　提示和故障排除

如果无线网络中一切均工作正常，您甚至不需要知道它的存在。您只需启动无线网络适配器，然后联机。

就像所有其他与计算机相关的事物一样，当一切都设置正确时就会很好地工作。但是基本设置通常隐藏在窗口、屏幕和对话框这三层之下，如果某些隐蔽的配置选项产生错误，网络连接就可能不会正常工作。

这一章包括了对一些常见问题的描述，以及如何解决这些问题的指导。

16.1　计算机没有检测到网络适配器

当您将一个 PCMCIA 或 USB 适配器连接到计算机，或者是先连接适配器再打开计算机时，Windows 操作系统将会自动检测到适配器。如果您使用的是一张 PC 卡，那么当 PCMCIA 控制器检测到它时，您将会听到“boodeep”的一声，然后时间旁的系统托盘就会显示如图 16-1 所示的 PC 卡图标。

图 16-1　当计算机的 PCMCIA 插槽中的一个设备激活时，会出现 PC Card 图标

如果 Windows 没有自动使您的网络适配器工作，那可能是因为它没有为您的 PCMCIA 套接字或适配器本身找到合适的驱动程序。Device Manager(如图 16-2 所示)将会为每一个目前不能正常工作的设备显示一个带有黄色惊叹号或红色 X 的图标。可以在带有惊叹号或 X 的列表上单击鼠标右键，然后在弹出的菜单中选择“properties”项来恢复设备或重新安装驱动程序。

如果根本就没有 PCMCIA 套接字或网络适配器的列表，您可以从随适配器一起提供的盘上安装驱动程序，或者从制造商的网站上下载一个新的驱动程序。

如果您的 Macintosh 机没有检测到 AirPort 适配器，可以尝试重装 AirPort 软件。

在 Linux 中，PC Card 需要有 PCMCIA 服务和无线扩展；在 Unix 中，您必须为您的网络适配器安装特定的驱动程序。

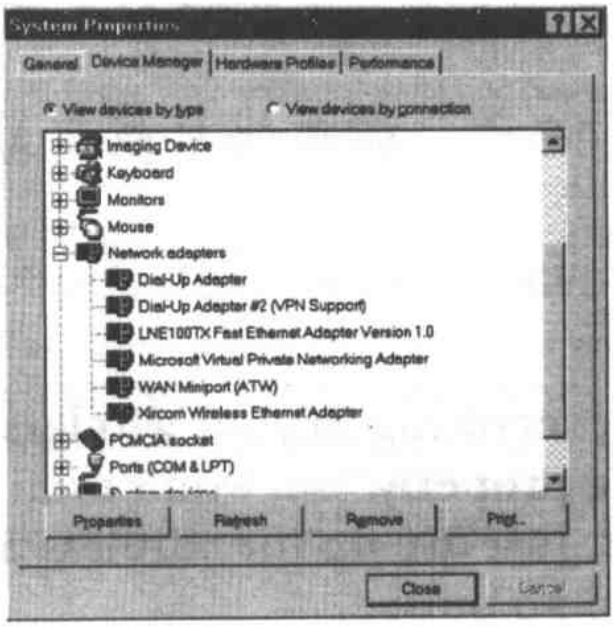

图 16-2　设备管理者程序识别没有正确工作的设备

16.2　无线配置程序没有运行

很多无线网络配置程序是为特定类型的网络适配器编写的，这些程序用来在启动时搜索匹配的适配器，如果没有找到，它们就会自动退出。因此，一个公司的配置程序遇到另一个公司的适配器时就很可能不工作。例外情况是那些使用多个品牌名称重新包装过的适配器和配置程序，如 Cisco 和 Xircom，或者 Orinoco 和 Apple，以及 Windows 或其他操作系统携带的配置程序。

因此，这个问题的解决办法就是安装一个专门为您将要使用的适配器编写的配置和控制软件。如果没有随适配器一起提供的 CD，您可以从制造商的网站上下载到您需要的程序。

16.3　即使不使用适配器，无线控制程序仍尝试运行

某些无线配置和控制程序在每一次计算机启动时都自动尝试加载，D-Link 适配器提供的软件在这一点上就显得特别讨厌，而其他的软件也完全可能这样做。对于桌面计算机而言，最好在启动时运行无线程序，因为它需要利用这些程序与某个局域网时时相连，但是对于一台通常工作在没有无线网络连接状态下的笔记本电脑来说，其意

义将大打折扣。

按照下列步骤在 Windows 上去除自动启动功能：

(1) 在 Windows 下的 Start 菜单上选择 Run。

(2) 在 Open 栏中输入 msconfig，单击 OK。

(3) 单击 Startup 标签显示每次启动 Windows 时自动运行的程序列表。

(4) 在该列表上找到无线配置程序条目，将同一行上的复选框的选择标记清除。

(5) 多数 Windows 系统都有其他几个不必要的自动启动程序。在保持这个程序打开时，找出其他不需要的程序，将它们禁用。

(6) 单击 OK，在 Windows 要求时重启计算机。

如果您已经从 Startup 列表上删除了几个程序，您可能会注意到 Windows 的启动速度较之以前快了很多。

即使现在每次启动 Windows 时配置程序不再运行，您还是可以在需要时启动它。您可能会在桌面或 Program 菜单中看到一个指向一个或多个无线程序的快捷方式。

16.4　计算机不能连接局域网

如果无法找到网络，检查如下这些项目：

- 确认无线网络适配器 PC Card 被牢固插入了 PCMCIA 插槽。
- 确认 USB 适配器和计算机之间的电缆两端都已插入。
- 打开无线配置程序，就确认 SSID 与您想要使用的网络接入点的 SSID 相匹配。
- 如果您正在使用一个接入点，就确认将您的网络适配器配置成基础结构网络；如果您正在试图直接连接到另一个无线适配器，就确认两个系统都被配置成 ad hoc 网络。
- 确认网络的 WEP 加密设置与适配器的设置相匹配。
- 确认 IP 地址设置是正确的。如果接入点或某个其他的 DHCP 服务器自动指定 IP 地址，就确认计算机的 TCP/IP 设置被指定为自动获得地址。
- 确认您的无线适配器的前缀长度设置与接入点的设置相同。一些配置程序把这个称为“Short Radio Headers”选项。
- 确认网络管理员已经在允许加入网络的设备列表中包含了您的网络适配器的 MAC 地址。不要相信适配器标签上印的 MAC 地址，它与实际指定给适配器的地址并不总是一样的。使用适配器的配置工具来查找真正的 MAC 地址，不要将适配器的 MAC 地址与它所连接的接入点地址相混淆。

16.5 计算机连接到了一个错误网络

如果在一个环境中，有多个无线网络的信号都在网络适配器的无线电接收范围内，那么适配器将会检测到全部这些信号。如果 SSID 选项被设置为加入“ANY”网络，则客户机将与本地信号最强的网络相连；如果配置程序包含其中有两个或更多 SSID 的列表，适配器就会按照列表指定的顺序搜索 SSID。

要将您的计算机配置成加入某个特定网络，可以更改工作组名称，以及在无线配置程序中修改 SSID 设置。无论是 SSID 还是工作组，都应与您想要使用的接入点的 SSID 相匹配。

遵循下列步骤，在 Windows98 和 Windows ME 中改变工作组名称：

(1) 在 Control Panel 上打开 Network 窗口。

(2) 单击 Identification 标签。

(3) 修改 Workgroup 栏内的名称。

遵循下列步骤，在 Windows 2000 和 Windows XP 中改变工作组名称：

(1) 在 Control Panel 上打开 System 窗口。

(2) 单击 Computer Name 标签。

(3) 单击 Change 按钮。

(4) 修改 Workgroup 栏内的名称。

大多数无线适配器在正常情况下都会自动扫描所有可用的无线电频道，从而搜索有用的网络信号。然而，某些配置选项允许用户将适配器锁定在单一频道上，如果该频道传送着其他某个网络，那么很可能适配器将会尝试加入该网络。所以，最好检查配置选项，确保适配器正在查看正确频道。

16.6 可以看到局域网，但是无法连上 Internet

多数局域网都会使用一个网关服务器将该局域网内部使用的 IP 地址转换成一个单独的 IP 地址，该地址在 Internet 中标识该局域网。为了建立一条 Internet 连接，您计算机上的 TCP/IP 网络配置设置必须指定网关地址和一个或多个 DNS 服务器的地址。

16.7 可以看到 Internet，但是看不到局域网上的其他机器

类似于 Norton Internet Security 中包括的客户防火墙程序在正常情况下会阻挡外面

进来的查看文件和目录的企图，这就防止了对计算机的非授权访问，但同时也挡住了局域网上的其他计算机，除非您特别指定允许来自这些计算机的访问(利用它们的 IP 地址)。防火墙控制程序应该包含一个允许您指出“受信任的计算机”或“允许本地访问”的功能(因各防火墙而异)，请参考防火墙程序文档以获得专门指导。

如果防火墙没有阻碍访问，那么有可能是您试图访问的计算机配置不正确，例如接入点没有识别出该计算机的 MAC 地址，或者该计算机关闭了文件共享。

16.8　信号强度微弱或者信号质量低下

假设在您的计算机可接收到的范围内有一个接入点，信号微弱可能是由您的网络适配器和接入点之间的某种障碍物所引起。为改善信号质量和信号强度，您可以尝试将适配器(和计算机，如果适配器在一张 PC Card 上)移到一个不同的位置。2.4 GHz 的无线电信号的波长非常短(因此得名“微波”)，所以，即使只是把适配器移动很短一段距离，也足以得到一个显著变化。

如果您使用的是 USB 适配器，在它位置的选择上您可以更加灵活。试着将它放到书架顶上或者别的能直接投影到接入点的位置，再试着调节适配器(或外置天线)的侧面，使它斜着而不是直立着，这可以使适配器天线的极性更接近接入点天线的极性。

16.9　找不到公共网络

在您的计算机能够连接到一个公用无线网络之前，您的网络适配器必须自动加入该网络的接入点。如果适配器没有自动加入网络，请检查下列配置设置：

(1) 确保配置实用程序被设置成认可该公用网络的 SSID。

(2) 确认 TCP/IP 环境被设置为接受 DHCP 服务器分配的 IP 地址。

(3) 在您尝试使用诸如邮件读取器的其他 Internet 客户程序之前运行您的 Web 浏览器。多数商业公用网络通过浏览器显示登录窗口，在您向他们标识自己(同时启动记账时钟)之前，他们不会建立任何其他连接。

16.10　不知道自己是否在网络范围之内

某些无线程序检测和显示附近所有网络信号的 SSID。所以为了检查某个信号，通常可以简单地插上适配器，然后运行状态程序。

要得到关于附近网络的更详尽信息，包括他们的 SSID，可尝试利用 Network Stumbler(可从 http://www.netstumbler.com 获得)来标识您的网络适配器所能发现的所有信号。Network Stumbler 是一个 Windows 程序，它并不适合于每种品牌的适配器，但如果与您的适配器是兼容的，那么它就是一个有价值的工具。尝试 http://www.wardriving.com/code.php 处的链接以获得其他操作系统上类似程序的信息。

16.11 网络速度慢

任何时候只要有一个网段慢下来，整个网络的性能都会受影响。这意味着一台超载的服务器或太多人同时尝试使用网络都可能使文件传输或下载速率降低。在网络的无线网段内，缓慢的性能可能由大量的网络访问要求或者操作于同一个频率上的其他无线网络或无线电服务干扰所引起。信号衰减和多路干扰同样能够导致无线网络数据传输速率降低。

为减小干扰，可尝试将接入点转移到一个距离原来频道至少 6 步以外的不同频道上。例如，如果您当前正在使用频道 2，那么可试着将接入点转移到频道 7。这需要访问接入点，所以通常只有网络管理员能够完成。

如果因为太多的用户同时在线而导致无线网络超载，那么可以增加更多使用不同频道的接入点。

如果接入点和某个单独网络客户机之间的数据传输速率慢，则试着将网络适配器的速率从“自动”变为 5.5 MHz，甚至于是 2 MHz。这看起来好像是违反直觉的——您如何通过降低传输速率来改善传输速率呢？——但该方法确实行之有效，因为使用高速链路的发射器将会重复发送每一个信息包，直到接收方确认已经收到了一个完全的副本。如果信号极端微弱，或者环境嘈杂，这就可能需要为每一个信息包尝试多次，即意味着每移动到下一个信息包都要花去几倍的时间。当您降低发送速率时，每个信息包都更容易理解，网络就可以不再需要不断重发它们。

16.12 可否用外置天线改善性能

一般而言，外置天线能够将无线网络的信号强度提升 15%或更多，因为它能够选择放置的位置，从而避开信号通路上的障碍物。外置天线既能附属在接入点上(在这种情况下，它可以提高到每一个网络客户机的信号强度)，也能附属在一个无线网络适配器上。假如您能在链路的两端都放上外置天线，那么总共的改进大约是 32.5%。

这是假设内置天线和外置天线有着完全一样的特性。如果外置天线有方向性，或者

它比内置天线有更多的增益，那么性能改善还会更高。另一方面，很多网络适配器和接入点都在一个“多样性”的系统中使用两个内置天线，该系统经常比较来自两个天线的信号，从中选择较强的一个。在一个嘈杂的环境里，一个多样性天线系统可能比单一天线更有效。

16.13　是否有改善性能的其他方法

从发射天线辐射出的能量通常在水平或者竖直平面里被极化，所以一个接收天线将会从有相同极性的天线处检测到更强的信号。换句话说，如果发送方使用了一个竖直天线，那么当接收天线同样竖直时，它将会检测到更强的信号；如果发送天线是水平的，接收天线同样应该是水平的。

在短距离内，极性不会对无线以太网链路的性能造成明显影响。即使两个天线具有不同的极性，它们仍然能够交换足以保持数据全速移动的信号。然而，当您试图从一个微弱或嘈杂的信号中提取出每一个可能的数据比特时，将两个天线放置成相同的极性就可以看到一些改进。

对嵌入在多数 PC Card 适配器上的内置天线来说，除非倾斜整台计算机，否则很难或不可能使它们移动，但是很多接入点的天线都安装在旋转轴上，所以很容易将天线从竖直位置切换到水平位置。

16.14　在移动到另一个接入点时，适配器失去了连接

通常认为，无线适配器会检测附近所有的接入点，并自动将自己的连接切换到一个具有清晰和强烈信号的接入点。然而，这种切换并非总是正确无误。有时，当来自最近一个接入点的信号渐渐变弱时，适配器只是简单地停止网络连接。如果发生这种情况，则可尝试关闭无线链路，然后再重新启动(先拔下无线卡，然后再插回去)，或者尝试重启计算机。

16.15　何处可以找到一份 802.11b 标准的副本

IEEE 标准是一些工程师为另一些工程师编写的，因此它们读起来并不特别有趣。然而它们是无线以太网的定义文档，所以您可能会希望查看它。它们可以从 http://standards.ieee.org/reading/ieee/std/lanman 处联机获得。

16.16　如何确定网络适配器的制造商

虽然包装上有标签，但很多无线网络适配器和接入点都是一些其他公司产品的私有标签版本。对一家公司来说，从别人处购买无线产品，并且将其添加到自己的商品目录要比自己从头设计制造容易得多。

一些出售私有标签版本适配器和接入点的公司会告诉您它们的制造者是谁，但也有很多销售人员坚称一切都是他们自己做的，即使不是这样，他们也会提供担保，所以您不需要担心什么。

作为一个用户或网络管理员，只要设备携有 Wi-Fi 证书，原始设备制造商(OEM)的名称对您来说应该没有什么不同。如果它通过了 Wi-Fi 测试，您就可以认为，它将会与您网络中的其他设备一起很好地工作。

然而，有时知道一个封装的 PC Card 包中究竟有些什么还是有帮助的。如果您将适配器用在一台运行 Unix 或 Linux 的计算机上，则制造商的技术支持人员可能会不知道到哪里寻找那些设备的正确驱动程序和配置工具；但当您知道里面究竟是什么组件时，您就可以自己找到驱动程序。作为一个网络管理员，有必要知道哪些适配器跟您已经在使用的相同，因为那样您就可以在手头上保留几个备用的，它们能同用户计算机上已经安装的驱动程序兼容。

那么，如何发现原始制造商的名称呢？您将不得不自己做一些侦查工作。凡是美国售出的能够发射无线电能量的电子设备都必须带有一个注册号，该注册号由联邦通信委员会(FCC)颁发。这种方法适用于无线电发射器(如无线网络设备)，也适用于大多数其他计算机组件，因为不管它们将要完成的功能是什么，它们都有发射无线电能量这个副作用。

大约每一个无线网络设备上都有一个 FCC ID 号。例如，图 16-3 显示了一张 ZoomAir PC Card 适配器上的标签，其 FCC ID 号是 BDNWLANPCCARD11。

FCC 在 http://www.fcc.gov/oet/fccid 中维护一个可查询的数据库，其中列出了每一个 ID 号，包括指向制造商当初申请注册时提供的所有技术展览品副本的链接。这些信息中的大部分都是烦人的技术资料，但如果您浏览一下，一般情况下就会在发现一些能够标识原始制造商身份的东西。

在这种情况中就很容易，其中一份测试报告指出“这张卡与 Intersil 卡相同”。这就是当您将这张卡安装到 Unix 系统上时所需要的信息，Intersil 卡使用 wi 驱动程序。

对于像我这样拥有一个废料箱，其中装满了看起来好像重要到需要保存、但却没有标签说明它们究竟适合做什么的古老计算机电路卡的人来说，FCC 数据库同样是一个强有力的工具。该数据库将每一张卡映射到一个列表，其中包括对这张卡的说明，甚

至于还可能包括一份用户手册的副本。有了制造商和型号，通常就可以找到一个提供更详尽细节信息的制造商 Web 站点。

图 16-3　所有无线网络设备在它的标签上都有一个 FCC ID 号

16.17　网络适配器或接入点所带的软件是否最新

和无线网络适配器一起提供的软件有两种存在形式：运行在与适配器相连的计算机上的程序，以及控制适配器自身的内部固件。运行于接入点上的所有软件都是固件。

无线联网硬件(包括其他大多数与计算机相关的产品)的制造商经常发布支持他们产品的软件的新版本。更新的软件可能包括产品出厂后才发现的一些故障的排除和对新操作系统的支持，以及额外的一些特性和功能(例如改进的加密技术)。检查制造商的 Web 站点，查看能得到些什么总是有用的。

安装新的配置和状态程序比较容易，只需要加载新软件来覆盖旧版本。多数情况下，制造商提供的软件是一个可执行文件，它能自动删除早期版本，并且运行一个完整的安装程序。最好阅读 README 文件，或者随下载包一起提供的其他指导。

更新固件就复杂得多。制造商总是提供详尽的指导，您应该尽可能严格遵循。在您更新一个接入点的固件之前，记得通知您所有的用户：网络将因维护而离线。

16.18 如何才能减少计算机电池的消耗

无线电发射器将电能转换成无线电信号，所以一台带有无线适配器的笔记本电脑上的电池能量会比一台同样的、但没有适配器的计算机下降得更快。幸运的是，您可以采取一些措施来将能量消耗保持在一个绝对最低的水平。

首先，在您不用的时候断开适配器。如果您在飞机上、火车上或任何其他超出一个无线信号范围的地方，或者您正在用计算机做的事情不要求网络访问，应从插槽上拿下 PC Card 适配器或拔掉 USB 电缆。如果您的计算机使用的是内置式无线适配器，那么也应当关掉它。

对任何 PC Card 上的插入式设备来说，这都是一个好建议。如果您不使用它，那么就拿掉它。任何时候只要插入计算机，调制解调器、以太网适配器和存储卡都会消耗能量，所以如果插槽是空的，电池就将会用得更久。

当使用无线网络适配器时，您可以使用作为 802.11 规范一部分的省电协议(Power Saving Protocol)来降低能量消耗。在适配器配置实用程序的某个地方，一系列能量管理选项可以指示适配器进入一个节能模式：

- CAM(Constantly Awake Mode，常醒模式)消耗最多的能量，但提供最快的响应速度。在这种模式下，适配器始终是开着的。只要接入点一得到进来的消息，它就接收它们。
- PSP(Power Saving Protocol，能量节约协议)模式消耗的能量较少，但同时响应速度也比较慢。在 PSP 模式下，适配器指示接入点将该网络节点的消息保存在一个缓冲区中，它自己则进入一个低能睡眠模式。在固定的时间间隔(每分钟数次)中，适配器将醒来，并且查询接入点有无消息。由于在接入点接收到每一个消息到将该消息发送给睡眠的适配器的时间之间有一个延迟，数据和消息通过网络将花费更长时间。

16.19 可否将接入点作为网桥使用

接入点就是位于无线网络和有线局域网之间的一座桥。如果单个接入点不足以到达无线网络服务的整个区域，则在有线局域网上连接额外接入点就可扩展覆盖区域。“无线桥”，即使用无线链路将两个局域网连接到一起，这是一个更特殊的功能。

很多接入点都将提供无线桥接作为一个选项，但它并不是基本特性集的一部分。如果您计划使用接入点作为网络之间的桥，则请在购买之前检查一下规范。您最好还是买一个单独的无线桥，而不是尝试使用一个通用无线适配器临时应急。

16.20　无线以太网发出的信号是否有危险

一些人相信关于蜂窝电话的安全性还没有定论，其他人则相信它们是一个严重的健康威胁。科学家和工程师们就此作了研究，并且发表了相应论文，在其中他们宣称已经证明了长期使用蜂窝电话可能——或者不可能——导致癌症和让牛奶变酸，或者有某些其他可怕影响。人们经常暴露在蜂窝电话和无线网络适配器所使用频率的电磁环境中，大多数研究过这一问题的组织都认为该频率在安全标准之内。反对者则相信那些标准太高了。

即使您认为蜂窝电话有潜在危险性，无线适配器中的无线电依然可能是更为安全的。首先，当蜂窝电话发送信号时，它距离用户的大脑只有一到两英寸，而无线适配器可能距离一步或更远(虽然它们也被称为“膝上型计算机”，大多数人还是在桌子上而不是在膝上使用它们)。非电离辐射(无线电波的别名)的效果按与距离的二次方成正比的速率下降，所以一个距离您大脑两英寸的发射器对您身体产生的影响将比一步之外的无线电大约强 36 倍，假如两个无线电信号在天线处的强度相同的话。

第二，蜂窝电话的无线电功率比一个无线适配器强 20 倍(0.60 w 比 0.03 w)，所以最终信号将强 700 多倍。

最后，无线电频率辐射对有机体的影响是累加性的——身体暴露在辐射中的时间越长，影响就越大。多数蜂窝电话只要连接被激活，它们就持续发送信号，而无线局域网是突发性的服务，它们只有在实际发送数据时才被激活。这意味着，一个无线适配器发送时间的总量只占蜂窝电话活跃时间的一部分。

因此，您的身体从一个无线网络适配器那里受到的辐射总量只占从一部蜂窝电话那里受到总量的极小一部分。

但是 Wi-Fi 信号就绝对安全吗？要获知 20 或 30 年以上的累积效果是如何还太早，因此没有人能做那种绝对的断言。但是所有证据都表明，它们很可能不会对您造成任何严重伤害。